MDM

MOBILE DEVICE MANAGER

Manual

Copyright 2013, 3CX Ltd. http://www.3cx.com
E-mail: info@3cx.com

Information in this document is subject to change without notice. Companies' names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of 3CX Ltd.

3CX Mobile Device Manager is a copyright of 3CX Ltd.

3CX is a registered trademark, and 3CX Mobile Device Manager and the 3CX logo are trademarks of 3CX Ltd. in Europe, the United States and other countries.

Version 7.1 – Last updated 15 May 2014

Manual Index

Section 1 - Introduction & Getting Started

1. Introduction, Benefits & Editions Available
2. Getting Started & Purchasing Mobile Device Manager

Section 2 - Enrol and Manage Devices

3. The MDM Clients
4. Device Management
5. Group Policies

Section 3 - MDM Features

6. Deploying Email and Exchange Accounts
7. Location Tracking
8. Security Features
9. Application Management
10. Managing Wi-Fi Settings
11. Remote Control
12. Messages and Directions

Section 4 - Account Management

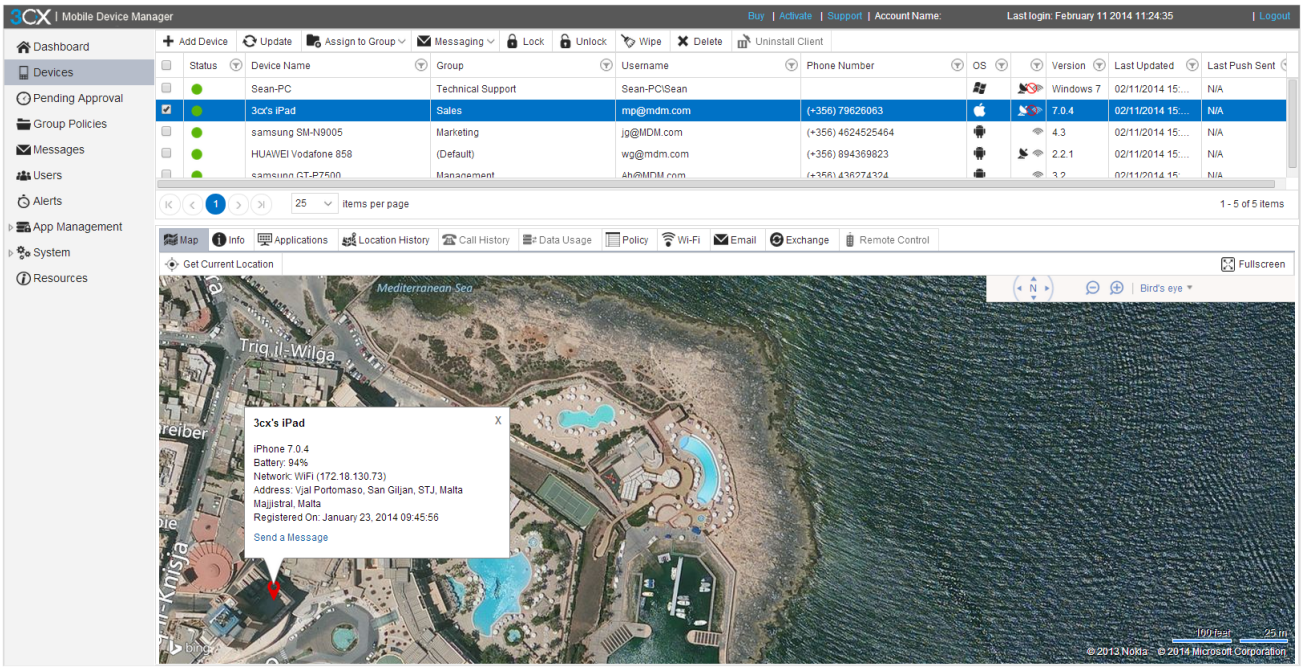
13. Alerts
14. System Node (Advanced Settings)

Introduction and Installation

What is 3CX Mobile Device Manager?

3CX Mobile Device Manager is a platform to manage, secure and track your mobile devices. Mobile devices connect to corporate applications and have access to or store confidential corporate data. As mobile devices are used by more and more staff, it is imperative that these devices are managed and controlled.

Benefits



Security

3CX MDM secures your mobile devices by:

- Enforcing a strong password policy.
- Being able to remote lock phones when they are being misused.
- Wiping corporate data off phones when they are lost or the employee leaves the company.
- Deleting corporate email accounts and the associated attachments downloaded and stored on the phone.
- Deleting corporate Wi-Fi networks and associated credentials stored on the phone.

Furthermore, 3CX Mobile Device Manager allows administrators to monitor for rogue / malware apps being installed on phones which could compromise corporate data. Also, with GPS and Wi-Fi tracking, you can retrieve a lost or stolen device.

Manage Email & Wi-Fi Configuration

Supporting users on configuring corporate email & Wi-Fi Network access on their smartphones can be cumbersome and time consuming process. With 3CX Mobile Device Manager, administrators can quickly push their email account details as well as Wi-Fi network names and passwords. This, saves the administrator time and increases security as its easier to change and manage these.

Monitor Data Usage & Calls

3CX MDM also helps companies monitor data usage and call costs. If employees aren't fully using their bandwidth or if they are using too much, the company can change the data-plan accordingly. Likewise, detailed call logs show administrators whether employees are making too many unnecessary calls.

App Deployment

3CX MDM helps companies manage the applications on the devices. By remotely installing apps, companies avoid the hassle of having to manually install them, which can take a lot of time, especially if employees need assistance. Applications that connect to confidential company databases that companies don't want to be made public, can be deployed without needing Google Play or Apple App Store, which can be a time intensive task to administer.

Reports show which apps are installed on each device, allowing easy monitoring for malware or inappropriate apps that waste company time, bandwidth or open up a company to legal issues. The version of approved apps that employees have installed can also be seen in order to ensure apps are all up to date.

Find & Track Devices

Track the routes your staff take to ensure they are using the most efficient routes when visiting customers and send them pinpointed locations via Google Maps. In case a phone is lost or stolen, it can be located.

Platform Independent

3CX MDM is platform independent. It works with Android smartphones and tablets, iOS based devices such as iPhones and iPads, Windows 7/8 devices and soon Windows 8 phones**.** Platform independence is crucial as few companies use just one type of device.

Cost of Manually Managing Devices in Business

Manually managing mobile devices is not an option. According to Gartner, companies spend on average $2,500.00 per year manually managing a single device. UK Internet Service Provider, Timico, conducted a survey which showed that 42.5% of companies in the UK spent up to 5 hours each day manually managing mobile devices. 14% of these companies spend one working day per week managing their devices.

ComputerWorld stated that a recent study revealed that two out of three companies are struggling in terms of not only defining but enforcing IT and business policies around mobile devices. The study also showed that 28% of companies surveyed reported a data breach because of a mobile device. The conclusion is that mobile device management is the best way to centrally secure and manage mobile devices.

Editions Available

3CX Mobile Device Manager is available as either a hosted or an on-premise edition.

Hosted / Cloud

3CX Mobile Device Manager is available in a hosted edition which allows you to manage your devices in the cloud. You can either pay your subscription fee yearly or every six months based on the number of devices that you are managing. This includes support, maintenance and system upgrades.

The hosted / cloud edition offers:

- Scalability, support from 5 to 5000 devices.
- Fully redundant data centers.
- High availability (HA).
- Easy to deploy.
- No significant investment.
- All software maintenance is handled by 3CX.

On Premise

3CX Mobile Device Manager can be deployed, managed and maintained completely on-premise as well. You can choose to use dedicated or virtualized hardware or install it together with other enterprise apps. You will retain full control of the data being collected. For more information see chapter 'Installing 3CX MDM On Premise'

On Premise customers purchase a perpetual software server license, based on the number of devices being managed. The perpetual software license includes one year of software updates. After the first year, you can purchase maintenance which ensures you continue to get free updates for the software.

Getting Started

Introduction

To get started with 3CX Mobile Device Manager, you will need to sign up online, invite users to install the mobile device clients and after installing the clients, you will be able to manage these devices online. Additional steps are required to manage iOS devices.

Sign Up for Your Account

The first step is to get an account:

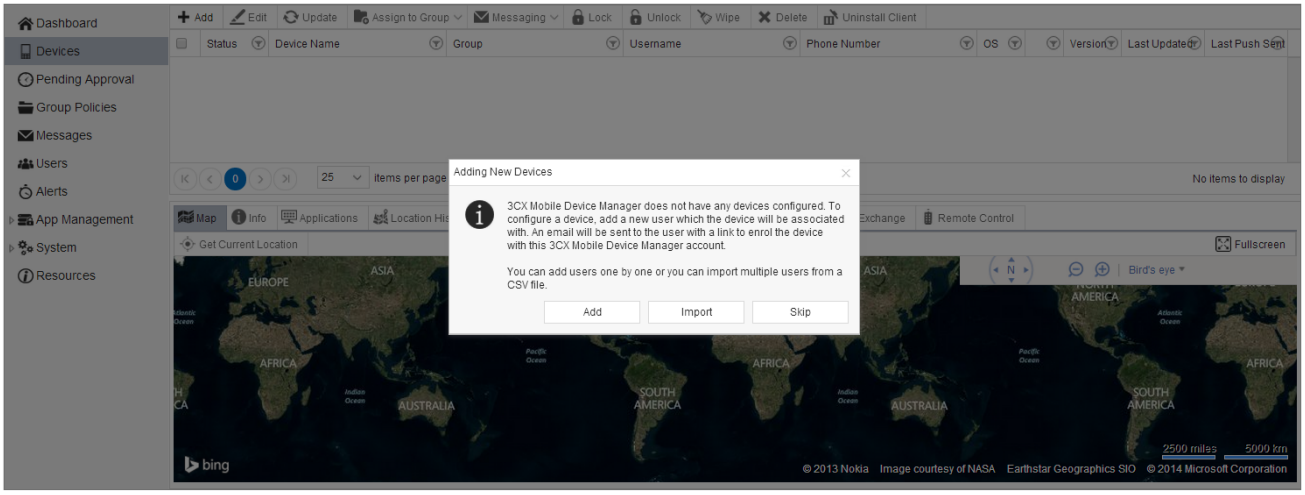
1. Go to http://www.mobiledevicemanager.com/signup/
2. Specify an account name. You will use this account name to enrol mobile devices and to log in to the 3CX MDM portal.
3. Specify your name and email.
4. Specify a password (to login to the portal).
5. Enter the CAPTCHA and click submit.
6. Activate your account by clicking on the link included in the welcome email sent to you.
7. You can now logon to the portal at http://admin.mobiledevicemanager.com by specifying your account name, email and password.

Apple iOS Users Note: Before you can manage Apple iOS devices, you must obtain an Apple PUSH cert. To do this follow this guide: http://www.mobiledevicemanager.com/faqs/configure-apple-certificate/

Adding Mobile Devices to Your Account

To manage mobile devices you need to install the 3CX MDM agent on these devices. The quickest way to do this is to specify the email of the device owners' and then send out an invite.

The invite email will contain an enrol link for the device, to guide users through the download and installation of the client as well as a configuration file which automatically configures the client with the account name.

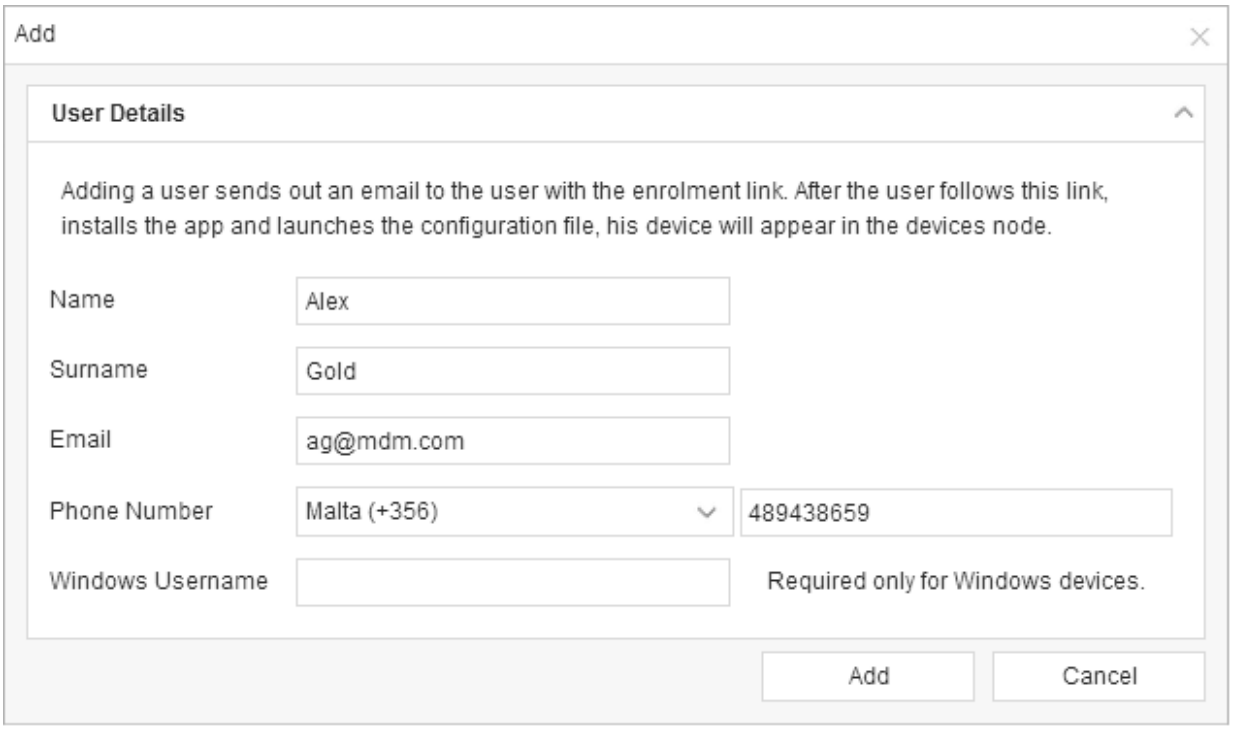


In fact, the first time you logon you will be prompted to import users or specify them one by one. Select 'Import Users' Or 'Add user'. You will be taken to the 'Users' node.

Adding Users One by One

To add users one by one:

1. Go to the ‘Users’ node and click on ‘Add User’.



2. When the add dialog appears, specify the user’s Name and Surname, Email Address, Country Code and Phone Number.
3. If you are inviting a user with a Windows laptop include the Windows Username. Press ‘Add’ when you have completed filling out these details.

4. Users will be sent an invitation email containing an ‘Enrol this Device’ link to enrol the device. The enrol process guides users through the download and installation of the client app as well as a downloadable configuration file (Windows and Android) which automatically

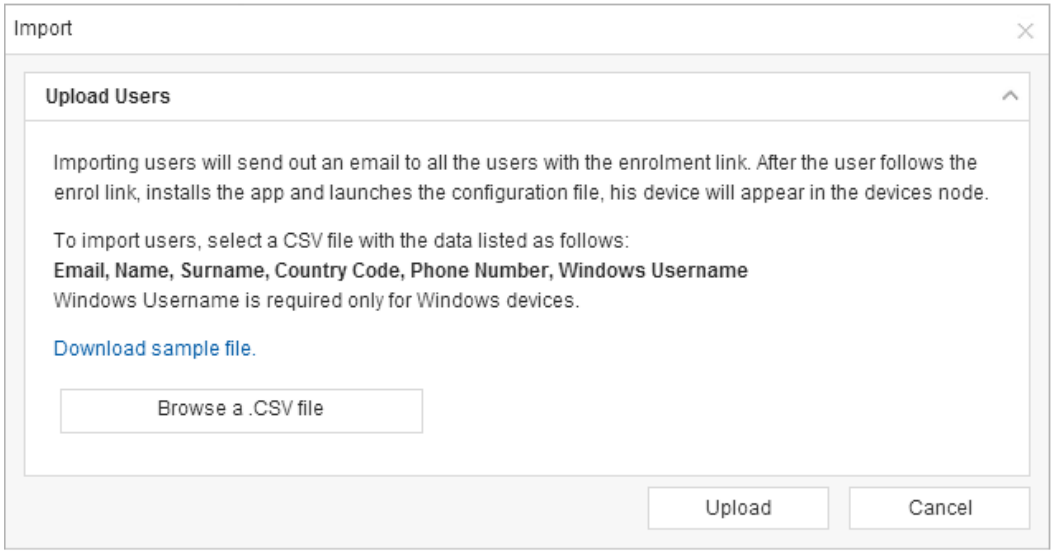
configures the client with the account and MDM server name.

5. The user must then accept rights and enable location tracking if required. More information here:
    a. Android: http://www.mobiledevicemanager.com/faqs/enroll-manage-android/
    b. Apple: http://www.mobiledevicemanager.com/faqs/enroll-manage-iphone/
    c. Windows: http://www.mobiledevicemanager.com/faqs/enroll-manage-windows/

Importing Users

If you choose to import users:

1. Export your list of users in the following format including the below text as column headers `Email, Name, Surname, Country Code, Phone Number, Windows Username`
2. Save the file in .CSV format.
3. Select 'Import Users' from the 'Users' node in the MDM Portal



4. Now specify the file using the 'Browse' button
5. Click 'Upload' to upload the file and import the users.
6. All users will be sent an invite mail containing an 'Enrol this Device' link to install the client and download the configuration file (Windows and Android) which will automatically configure the client with the account and MDM server name.
7. The user must then accept rights and enable location tracking if required. For more information:
    a. Android: http://www.mobiledevicemanager.com/faqs/enroll-manage-android/
    b. Apple: http://www.mobiledevicemanager.com/faqs/enroll-manage-iphone/
    c. Windows: http://www.mobiledevicemanager.com/faqs/enroll-manage-windows/

Assigning the User to a Device (iOS only)

Important: Before assigning a user to a device you need to have that device added to your account first. To add an iOS device to your account follow the Enrol process.

In the case of iOS devices, you need to create a user and then assign the user to the device unless you have configured the device by clicking the 'Enrol this Device' link from the 3CX MDM invitation email in which case the user is automatically assigned to the iOS device. If you added the device directly from https://admin.mobiledevicemanager.com/enroll you will need to assign the user manually to the iOS device.

Note however, that even without the user name, location services and MDM functions will still be available. For android phones this step is not required as the google user name is used to automatically assign the user.

To assign a user to an iOS Device:

1. Add the user that you want to assign to the device by going to the users node and pressing the 'Add User' button (if you already have a user in your users node that you want to assign to your iOS device go to step 3 directly)
2. Fill in the user's personal details and press 'Add' to add the user.
3. Go to the devices node and select your iOS device. From the topmost toolbar, click the 'Edit' button.
4. Click on the '(Anonymous)' field next to the Username and from the drop down select the user that you want to assign to your device.
5. After you select the user press 'Save' to assign that user to your iOS device

Note: Alternatively, open the invitation email sent when a user was created from an iOS device and click 'Enrol this Device' to automatically assign that user to that device and approve the device.

Approving the Device

If a user has installed the profile without having been invited first (from https://admin.mobiledevicemanager.com/enroll), then the mobile device will appear in the 'Pending Approval Node'. In this case, you need to approve the device first from the Pending Approval node, which once completed shall prompt the user to install the 3CX MDM client app.

Purchasing 3CX Mobile Device Manager

3CX Mobile Device Manager is free for up to 5 mobile devices. If you need to manage more mobile devices, you can purchase a license for 6 months or 1 year, for your desired number of mobile devices. Full pricing information is available here:
http://www.mobiledevicemanager.com/Pricing/

You can purchase 3CX Mobile Device Manager license from any 3CX reseller. You will find a list of 3CX partners here:
http://www.3cx.com/ordering/Find-reseller/

Activating Your 3CX Mobile Device Manager License

If you have purchased a 3CX Mobile Device Manager license, you can activate it as follows.
Step 1: Log in to 3CX Mobile Device Manager - https://admin.mobiledevicemanager.com.
Step 2: Click on **Activate** (top middle section of the screen) or select the System node > License Activation and paste in your License key.

The MDM Clients

Introduction

3CX Mobile Device Manager requires its MDM clients to be installed on the mobile devices for all functions to work correctly. Because MDM functions differ for each platform the steps to install the clients differ to some extent. In addition, some functions are not available on all platforms because of limitations or rules imposed by the vendor.

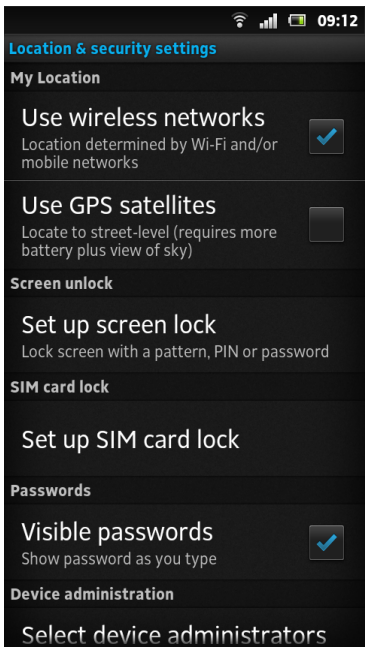
This chapter discusses the clients for each platform - the details of their installation, the process of uninstalling and their limitations.

The Android Client

Enrolling Android Devices (Without Invite)

To install the 3CX MDM Android agent without sending an invite via email:

1. Point your Android device browser to the Enrol portal URL: https://admin.mobiledevicemanager.com/enroll
2. Specify the 3CX MDM account name and click ‘Enrol’ (Click ‘Enrol this Device’ in the invitation email to skip steps 1 and 2)
3. Tap the ‘Install Android Client’ button to open the 3CX MDM Google Play store page and install the client.
4. Go back to the Enrol portal and tap ‘Download Configuration File’ button to download the 3CX MDM account configuration file.
5. Tap the downloaded file to automatically configure the client with the account name.
6. Enable location tracking from Settings > Location. (Settings > Location Services, Settings > Location & Security are also used depending on the Android version and phone manufacturer) Click on the Settings button in the 3CX MDM app to have 3CX MDM take you to the correct setting immediately. Enabling ‘Use wireless & mobile networks’ is sufficient to track a device.



7. Approve the phone from the 3CX MDM portal.
8. For more information: http://www.mobiledevicemanager.com/faqs/enroll-manage-android/

Android Client Limitations

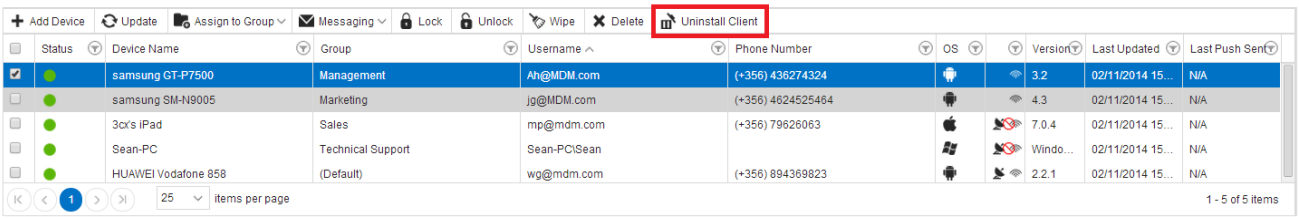
The Android Client has the following limitations:

- Cannot Specify Minimum Password Length.
- Cannot Force Change Password Every x Number of Days.
- Cannot Specify Max Incorrect Entries Before Device Wipes Automatically.

Uninstalling the Android Client Automatically Through the MDM Portal

To uninstall the Android client automatically:

1. Log in to the MDM portal.
2. Go to the 'Devices' node.
3. Click on the device that you want to uninstall the client from.



4. Select 'Uninstall Client' from the MDM menu.You will receive a confirmation message and the client will be uninstalled from your Android device.

Uninstalling the Android Client Manually

To uninstall the Android client, please follow these steps:

1. Go to your Android phone's Settings' menu.
2. Select 'Security'.
3. Scroll down to 'Device Administrators' and tap to open.
4. De-Select 3CX MDM.
5. You will get a dialog indicating the 3CX MDM rights. Press 'Deactivate'.
6. You will get a warning that disabling the service will leave your device unprotected. Press ok to confirm the MDM administrator account deactivation from your phone.
7. After that you should see that the 3CX MDM is deactivated on your device administrator's menu.
8. Leave the 'Security' settings and on the main settings page tap the 'Applications manager'.
9. Find the 3CX Mobile Device Manager entry, tap to open the App info tab and press 'Uninstall' to begin removing the application. Press 'OK' at the confirmation dialog.
10. 3CX MDM will be removed from your Android device.

The Apple iOS Client

Enrolling iOS Devices

To manage iOS Devices, such as an iPhone, iPad or iPod, follow the 'Enrol' process to install and configure the iOS MDM client and related profiles:

1. Make sure you have obtained an Apple Push Certificate. Follow this link for detailed information on how to do this: http://www.mobiledevicemanager.com/Faqs/Configure-apple-certificate/
2. Install the 3CX MDM agent app by following the 'Enrol' process. For more information on how to do that see here: http://www.mobiledevicemanager.com/faqs/enroll-manage-iphone/
3. Point your iOS device browser to the Enrol portal URL: https://admin.mobiledevicemanager.com/enroll
4. Specify the MDM account name and tap 'Enrol' (Click 'Enrol this Device' in the invitation email to skip steps 3 and 4).

5. Tap ‘Install Profile’ and approve the installation of the MDM profile.
6. Enable location tracking from iPhone Settings > Privacy > Location Services
7. Approve the phone from the 3CX MDM portal (Skip this step if enrolled from the invitation email link).
8. Once approved, accept the installation of the 3CX MDM iOS client which appears on the device.
9. Assign a user to iPhone (not required if enrolled from the email invitation link). This can be done by creating a user in the users node and then assigning that user to the phone from the Device > Edit button.
10. You can also configure the Notification Settings for the iPhone Agent. This is done by going to the iPhone Settings>Notifications>Select 3CX MDM , from there you can choose:
    a. None, if you do not want to send any push notification settings to users.
    b. Banners, if you want the notifications to be removed automatically after a while without the user intervention.
    c. Alerts, if you want each push notification to wait for an action from the user before proceeding.

Note: iOS 6 and below users shall not be prompted to install the 3CX MDM client app once approved.

Uninstalling the iOS Client

To uninstall the iOS client, please follow these steps:

1. Find the MDM Program icon on your iOS device.
2. Press and hold the icon until you see the icon vibrating and a small ‘x’ appears on its left corner.
3. Tap the ‘x’. A dialog will appear warning you that deleting 3CX MDM will also delete all of its data.
4. Press Delete to confirm.
5. The 3CX MDM iOS client will be uninstalled from the device.

To Remove the MDM profiles please follow the below steps:

1. Locate and press the Settings icon on your iOS device.
2. Go to General > Profiles
3. Select the 3CX Mobile Device Manager profile and press the remove button.
4. Press remove on the Remove Profile dialog

Further, for a more detailed explanation, follow this guide on how to uninstall the 3CX MDM Agent and Profile from your iPhone or iPad -http://www.mobiledevicemanager.com/faqs/removing-mdm-profile-from-iphone/

iOS Client Limitations

- Tracking via Mobile Networks is currently not supported.
- Remote Lock and Remote Wipe via SMS is not currently supported.
- Cannot remove applications that were installed by the user before the user installed 3CX MDM on the iOS device.
- Install app via setup uploaded to the MDM Server is not currently supported.
- Cannot Force an Alphabetic password.
- Cannot change network settings configured by phone user.
- Cannot automatically update server when the user changes the configured networks on the phone.

The Windows Device Client

Enrolling Windows Devices

To manage Windows 7/8 laptops, follow the below process:

1. Point your Windows laptop default browser to the Enrol portal URL: https://admin.mobiledevicemanager.com/enroll
2. Specify the MDM account name and click ‘Enrol’ (Click ‘Enrol this Device’ in the invitation email to skip steps 1 and 2).
3. Click the download link to download the 3CX MDM Client app.
4. Double click on the downloaded file to start the installation on your laptop.
5. Select the installation folder that you want to install the agent to and then press ‘Next’ and further ‘Install’.
6. The file installation will begin and the necessary files for your Mobile Device Manager agent to start will be installed on your machine. Press ‘Finish’ at the next screen to complete the setup.
7. Go back to the Enrol portal and click the configuration file link to download the 3CX MDM account information and click to run this file which shall automatically configure the MDM client app.
8. Log in to the 3CX MDM Portal and approve your laptop from the 'Pending Approval' node (Skip this step if enrolled from the invitation email link).

Uninstalling the Windows Client

To uninstall the Windows client please follow the next steps:

1. Press the ‘Start’ button, then go to ‘Settings’, click on ‘Control Panel’ (Windows 8 users should just search for ‘Control Panel’).
2. Go to ‘Programs and Features’, double click and wait until the installed programs list is populated.
3. Find the ‘3CX Mobile Device Manager Client’ on the program’s list and double click to uninstall
4. Press ‘Yes’ at the confirmation dialog asking if you want to uninstall this product.
5. The 3CX Mobile Device Manager client will be uninstalled from your Windows machine.

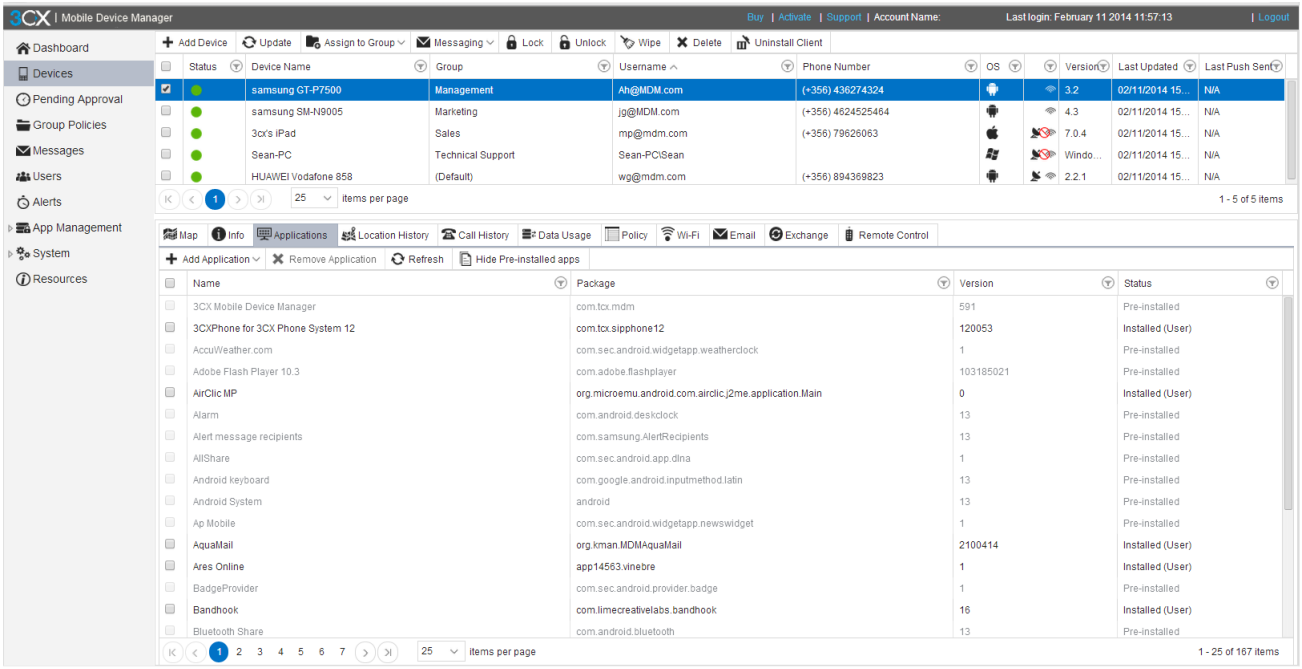
Windows Client Limitations

- Messaging is not currently supported.
- Commands are not executed immediately as in the Android client. The commands are executed every 15 minutes (or less depending on the 'Client Update Interval' setting).
- The ‘Remote Wipe’ command deletes and overwrites all files in the user’s Library (including the Documents, Pictures, Videos and Music folders and anything else that is in the library).
- Some applications may not be detected by the client if they are installed per user account and do not use the Windows installer.
- The current user password cannot be checked against the Password Policy for compliance, despite the fact that the 'New Policy Applied' message is shown to the user.
- Password Policies cannot be applied if the device is connected to an Active Directory
- Whitelists and Blacklists are currently not supported.
- Remote Application Deployment is currently not supported.

Device Management

Introduction

The main screen in Mobile Device Manager is the ‘Devices’ screen, which shows all registered mobile devices, their status and their configuration options.



Device Listing

The information column headers allow MDM account administrators to filter the information displayed within the 'Devices' screen.

The following information columns are available:

- Status - Shows whether the client is offline or online.
- Device Name - Shows the device name, obtained automatically from the device itself.
- Group - Shows the name of the group to which the device is assigned.
- Username - The user assigned to the device. For Android devices, the user is obtained and assigned to the device automatically and for Windows devices the Windows Username is used (for example: computer_name\username). For iOS devices, you must create a user from the users node and assign it to the device from the Device>> Edit button.
- Phone Number - The phone number associated to the device. In many cases the number can be obtained automatically. In some cases you need to specify it manually.
- Version - Shows the version of the OS.
- OS - Shows OS type, i.e. Android, iOS or Windows.
- The type of connection providers that the phone has to the MDM (GPS, Wi-Fi)
- Last Updated - Shows the date and time MDM last communicated with the device.
- Last Push Sent - Shows the date and time MDM last sent a PUSH request to contact the device.

Performing Actions on the Device

Selecting a device will allow you to perform the following actions:

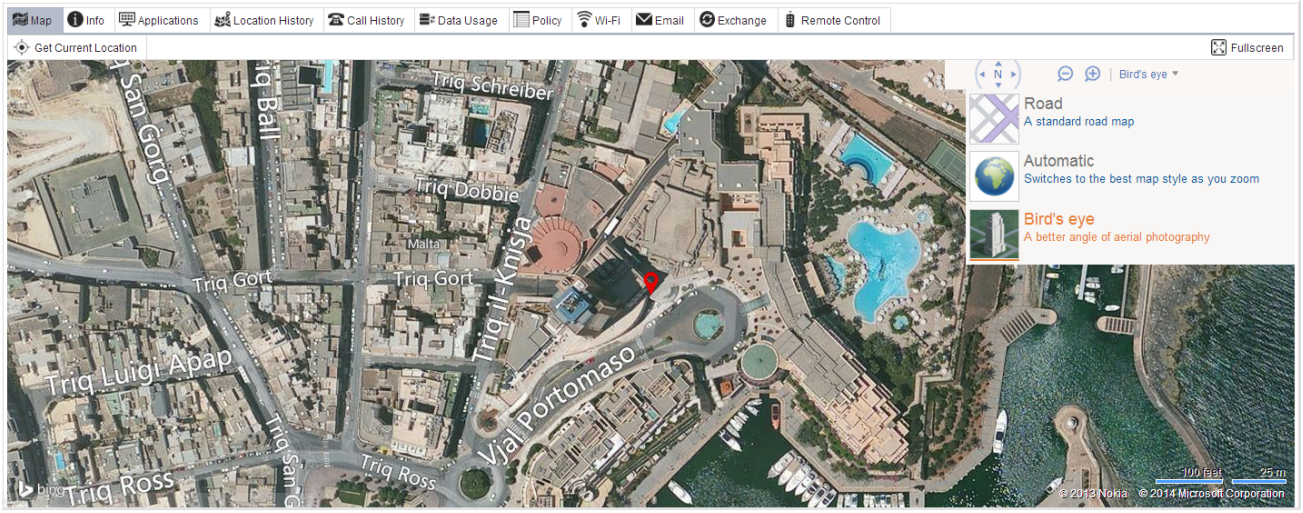
- Update - This will have MDM send a push request in order to obtain the latest location.
- Assign to Group - Assigns the device to a group, for easier management.
- Messaging - Allows you to send a text message, a URL or a location to the device.

- Lock - Performs a Remote Lock on the device.
- Unlock - Performs a Remote Unlock on the device.
- Wipe - Performs a Remote Wipe on the device.
- Delete - Deletes the device from your MDM account.
- Uninstall Client - Uninstalls the client from your device (only valid for Android and Windows devices).

Device Information and Configuration

Selecting a device allows you to go to any of the tabs below to configure it or obtain information about the device.

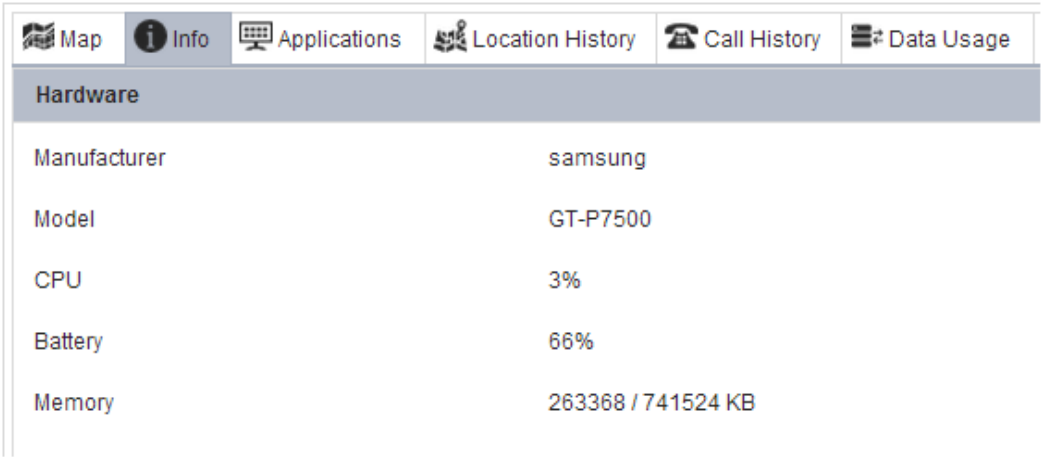
Map Tab



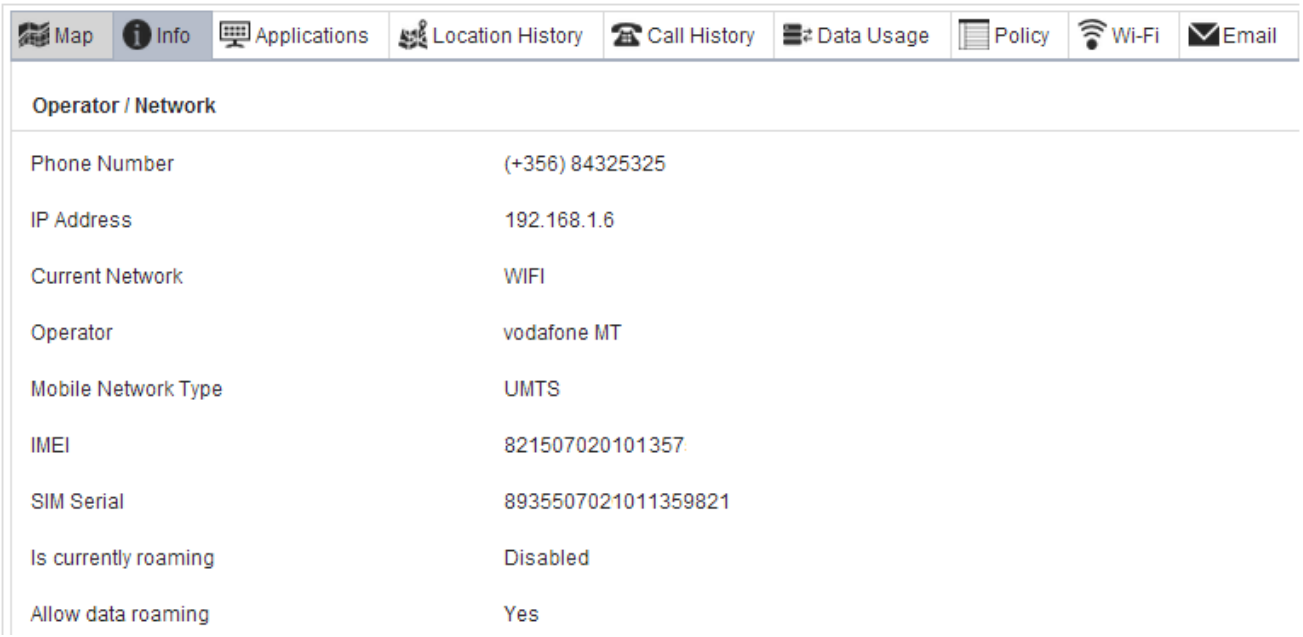
The map tab shows the last obtained location of the device, offers different view types and also supports multiple selected devices positioning simultaneously.

Info Tab

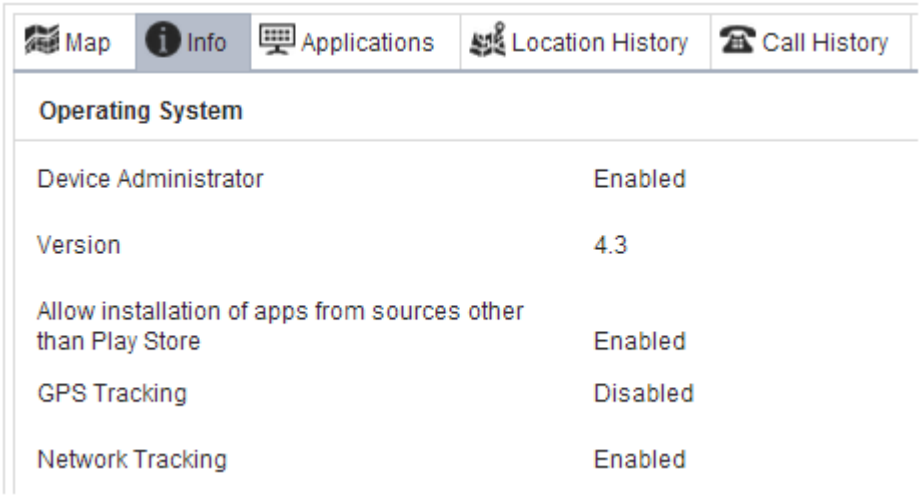
The info tab shows information obtained from the device. It is divided into four sections: Hardware, Operator / Network, Operating System and MDM Client



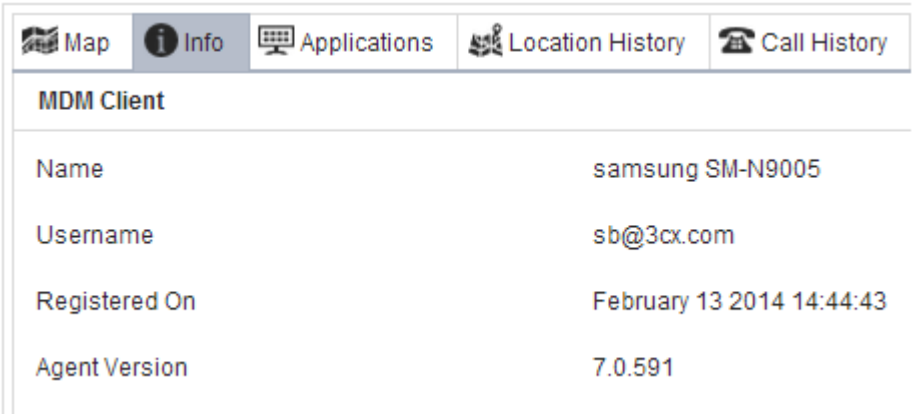
The hardware section contains information about the device, including the Manufacturer, the Model name, CPU usage, Battery level and Memory available. Note that IOS based devices also display the device UDID.



The operator section shows the mobile device's Phone Number, its IP Address, how it is connected to the Current Network, the telecom operator and its Mobile Network Type, the IMEI number, the SIM Serial number and whether data roaming is allowed and enabled.

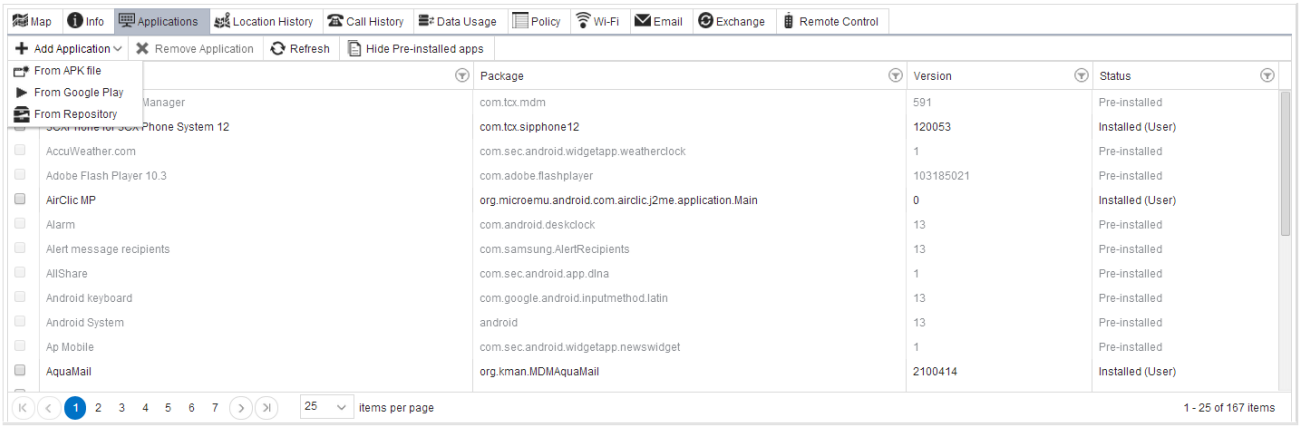


The Operating System section shows whether the Device Administrator is enabled on the device, the OS version that is installed on the device, whether the agent will allow installation of non-market apps, whether GPS tracking is active and whether Network tracking is active.



The MDM Client section shows the name of the device, the user name that is associated with the device, the date that the device was registered on MDM, and the version of the MDM agent that is running on the device.

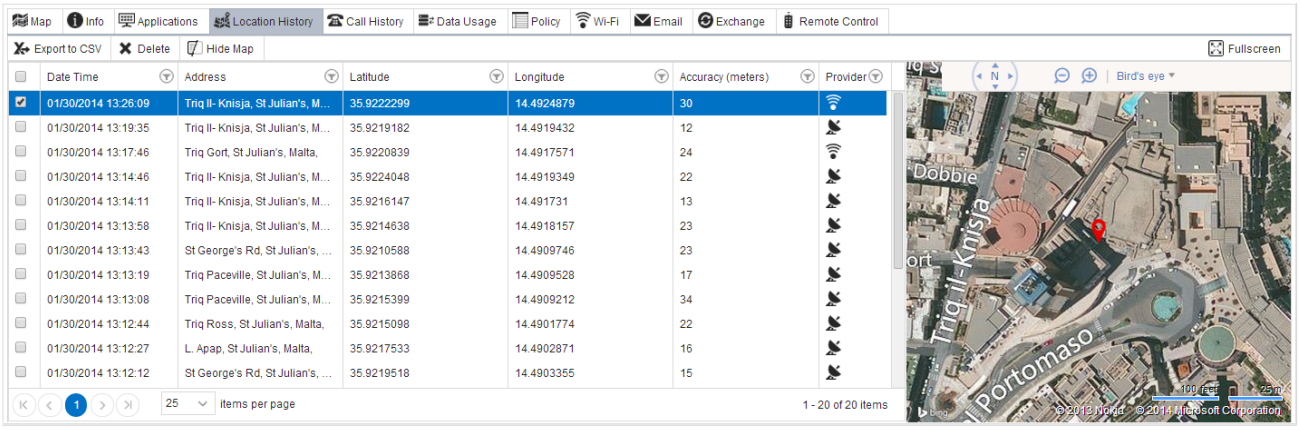
Applications Tab



The Applications tab shows all the installed apps on the device and with regards to Android based devices, allows you to install apps via Google Play, from your App repository or by specifying an APK file directly. Furthermore, for iOS based devices, you may select to install apps from the app store and also from your app repository. You can also remove apps from here.

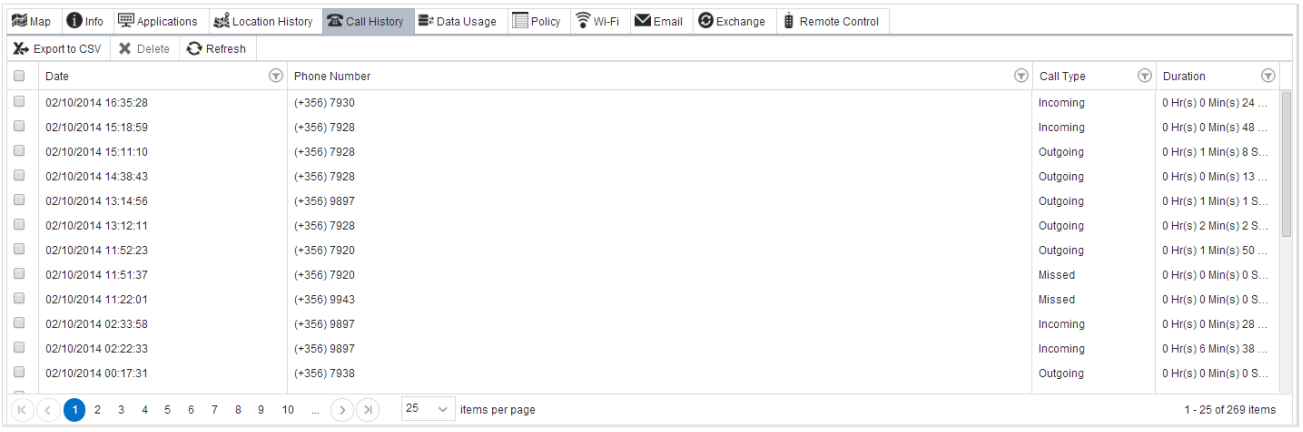
The screenshot above shows apps installed by the user (‘Installed (User)’) as well as apps that are pre-installed by the manufacturer and several other statuses as described below. You can hide the pre-installed apps by clicking ‘Hide Pre-installed Apps’ and further show pre-installed apps by clicking 'Show Pre-installed apps'.
Note: You cannot uninstall the applications that are pre-installed on your device by the manufacturer.

Location History Tab



The Location History tab shows the whereabouts of the device you have selected. It will show the date and time the location was resolved, the Latitude and Longitude, along with Address, Accuracy and the provider (GPS or Network) that was used to obtain the position.

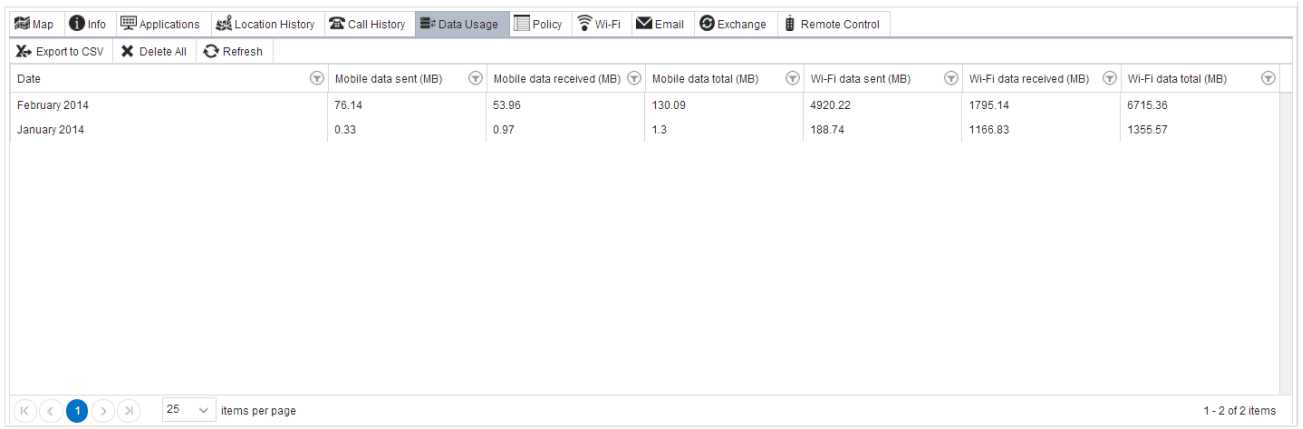
Call History Tab



The Call history tab shows all calls made on the device. You can export the data to CSV for further analysis in another application.

Note – This tab is not available for iOS based devices.

Data Usage



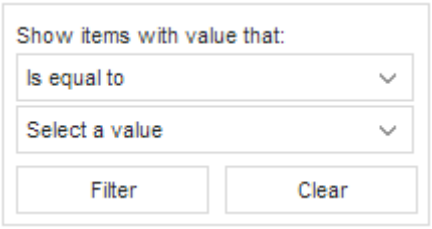
The Data usage tab shows both mobile and Wi-Fi data consumption by the selected device, per month. You can export the data to CSV for further analysis in another application.

Policy, Wi-Fi, Email and Exchange Tabs

The Policy, Wi-Fi, Email and Exchange tabs are discussed in their respective chapters. If you make configuration changes here, they will only be applied to this device. The Group Policy will be overridden by these settings.

Information Column Filters

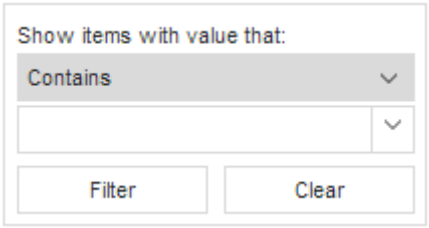
Further filter the information displayed within the above mentioned tabs to produce meaningful results. Filters are located in the information column header fields and allow filtering according to the examples below.



The above filter box allows you to filter based on the values displayed within a column. For example, the status column, located within the applications tab accommodates for the following values- Online Devices, Offline Devices or Disabled devices etc.

Additionally, you may apply the following conditions to the value selected and click ‘Filter’ to apply:

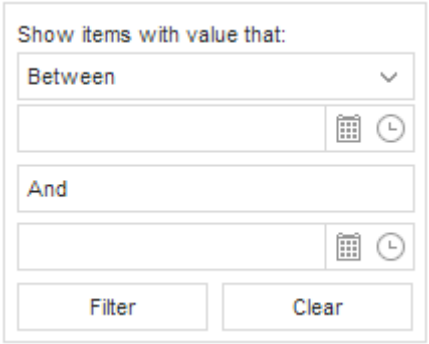
- Is equal to
- Is not equal to



This filter contains a textbox which filters values based on the data type accepted by the selected column. For example, the phone number column accepts numbers, brackets and the + symbol.

Further apply the following conditions to the value entered and click ‘Filter’ to apply:

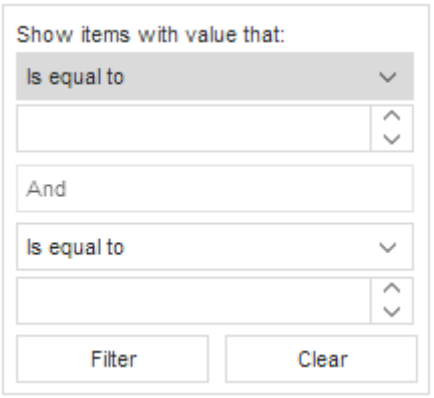
- Contains
- Is Equal to
- Starts with
- Ends with



The above filter contains two text fields to manually enter a date and time range, or alternatively, click the calendar and time buttons to select a date and time and further apply filtering on the selected range as per the below conditions:

- Between
- After
- Before
- Is equal to

Note: You may also enter a single value within the topmost textbox (date and time) and further filter using the above conditions.



The above filter contains two text boxes which allow you to define a range to filter within, based on the data type accepted by the column and further apply filtering on the entered value as per the below conditions:

- Is equal to
- Is not equal to
- Is greater than or equal to
- Is greater than
- Is less than or equal to
- Is less than

Note: You may also enter a single value within the topmost textbox (accepted data type) and further filter using the above conditions.

Group Policies

Introduction

To be able to manage a large number of mobile devices, Mobile Device Manager incorporates the ability to set policies to groups of mobile devices. You can configure different policies for each group of devices, and this will be automatically applied to each device assigned to the group. In addition, you can override a group policy for a particular device.

Default Group

By default, all devices are assigned to the ‘Default Group’ and the default group policy is applied. The default group policy will also push out the AquaMail for MDM app so that you can control email settings on Android Devices.

Once you assign a device to another group that you have created, the default policies will no longer apply.

Grouping Mobile Devices

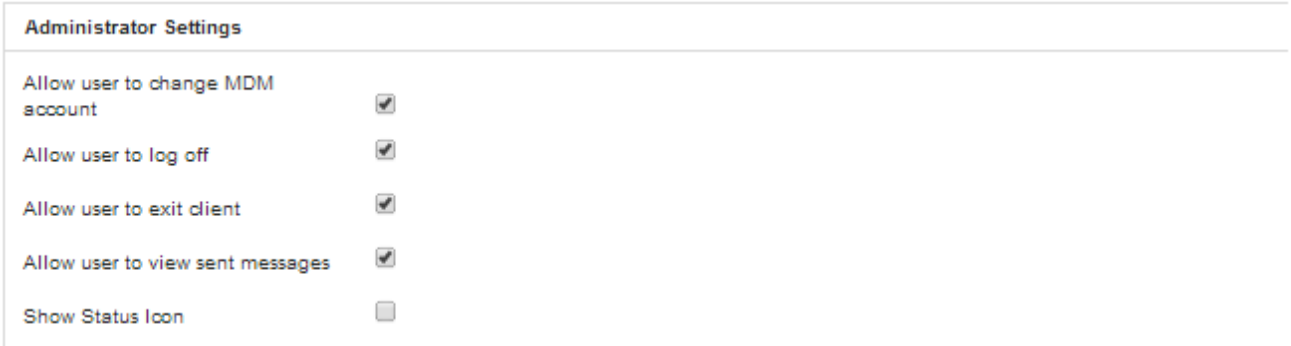
The first step is to group your mobile devices, for example by department. To group your mobile devices:

1. From the 'Devices' node, select the devices you wish to group.
2. Click 'Assign to Group'. Select whether you want to assign the devices to an existing or a 'New Group'.
3. The devices are now grouped, and they will show up as a group under the 'Group Policies' node.
4. You can select the group from the 'Group Policies node'. Any changes and settings that you make will be applied to the entire group.

Policies for Android Devices

In this tab you can define settings that should be applied to all Android phones in the group such as:

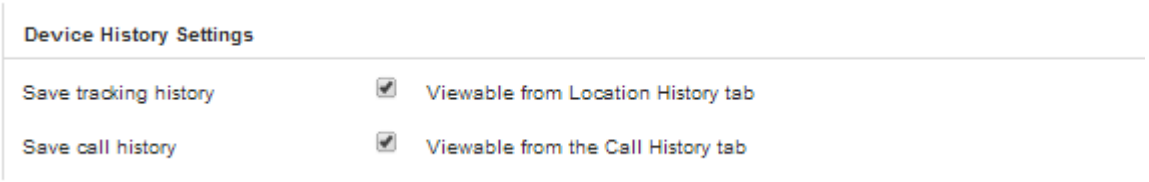
Administrator Settings



- **Allow user to change MDM account** - This option allows a user to logoff and logon to another MDM account. This option is turned off by default and only recommended for testing purposes.
- **Allow user to log off** - This allows a user to logoff from the MDM server. Should only be used for testing purposes.
- **Allow user to exit client** - Allows a user to close the MDM client. Only to be used for testing purposes.
- **Allow user to view sent messages** - Shows the messages sent and received via MDM on the user’s phone.

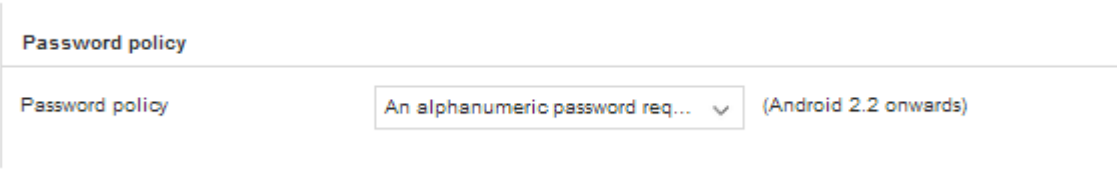
- **Show Status Icon** - This option will show the status icon as connected or disconnected on the user's phone. Mainly to be used for testing purposes.

Device History Settings



- **Save tracking history** - Saves the tracking history of the devices in the group
- **Save call history** - Saves the call history of the devices in the group

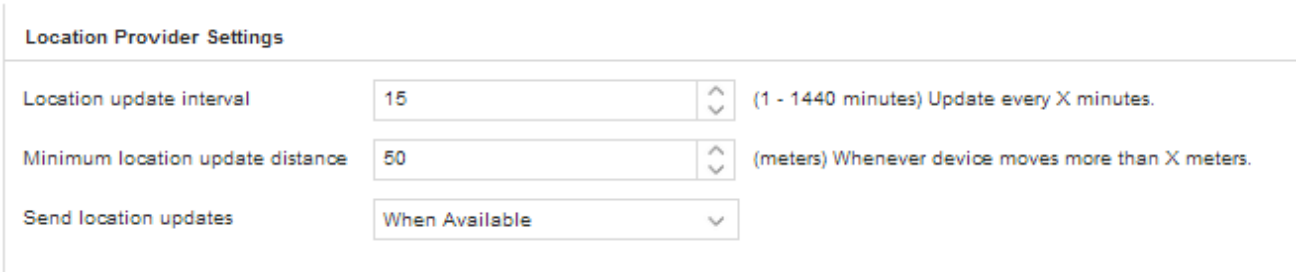
Password Settings



This section allows you to alter the Password Policy settings. You can select:

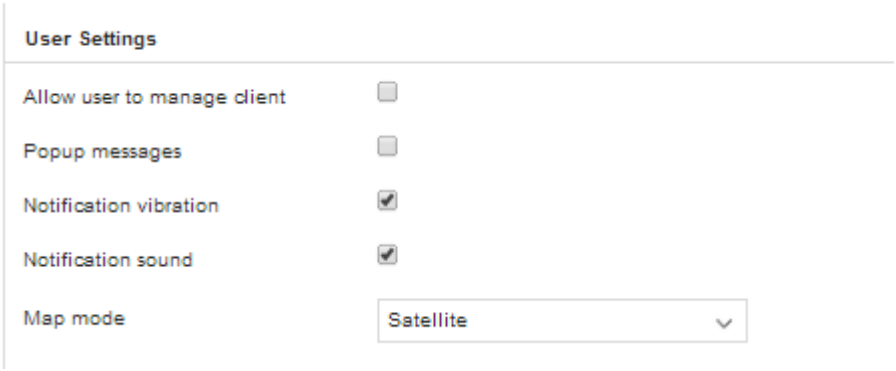
- **No password policy enforced**.
- **Password required (Any)**.
- **At least a numeric password required**.
- **At least an alphabetic password required**.
- **An alphanumeric password required**.

Location Provider Settings



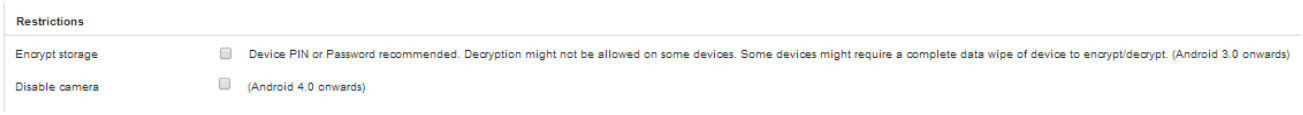
- **Location update interval -** Specifies the time interval (in minutes) that the phone will send a location update to the server,
- **Minimum Location Update Distance** - Specifies the minimum distance that a device should move to trigger a location update.
- **Send Location Updates** - This setting defines how location updates are collected and sent to the server. The following options are available:
    - **Force Network only** - This option sets the device to send location updates via Network only
    - **Force GPS / Network** - This option sets the device to send location updates via GPS OR Network,
    - **Force GPS only** - This option sets the device to send location updates via GPS only
    - **When Available** - The device will send both network and GPS position updates to MDM, depending on which are enabled and available on the device. If both are available, MDM subsequently updates the location history with the position possessing the highest accuracy.
    - **Off** - Turns off location tracking

User Settings



- **Allow User to Manage Client** - Enables configuration options on the MDM client > Settings, such as:
    - Popup Messages
    - Map Mode
    - Send Location Updates
    - Notification Vibration
    - Notification Sound
- **Popup Messages -** Display message as a pop up immediately.
- **Notification Vibration -** The phone will vibrate when a message is received.
- **Notification Sound -** A notification sound will be played when a message is received.
- **Map Mode** - When sending directions with messages, this will show the option as either a traffic or a satellite image.

Restrictions

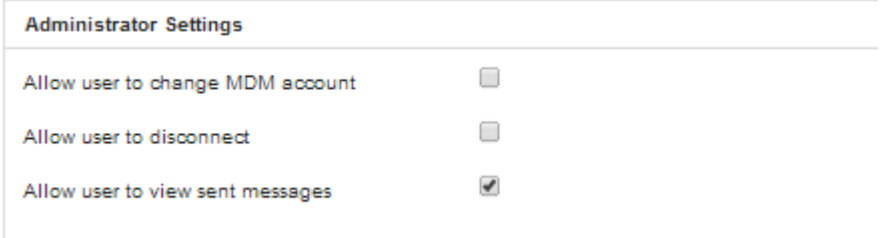


- **Encrypt Storage** - This option encrypts the information on your devices , note that decryption might not be allowed on some devices and that a complete data wipe might be required to decrypt/encrypt, use with caution
- **Disable Camera** - Disables the cameras of the devices in the group

Policies for iOS Devices

In this tab you can define settings that should be applied to all iOS based devices in the group such as:

Administrator Settings



The administrator options are similar to the Policy Options for Android phones:

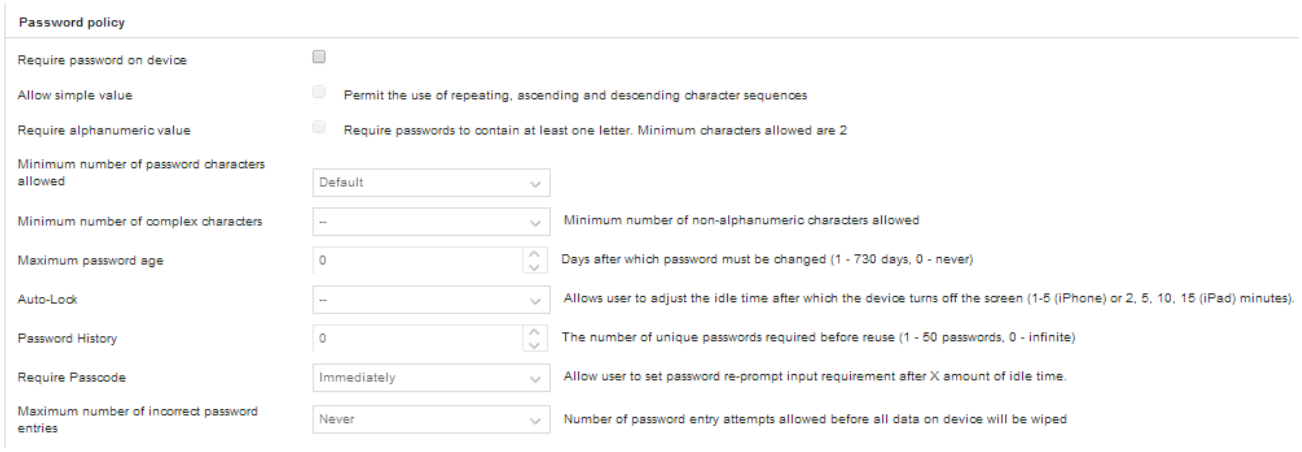
- **Allow User to Change MDM Account** - This option allows a user to logoff and logon to another MDM account. This option is turned off by default and only recommended for testing purposes.

- **Allow User to Disconnect** - This allows a user to logoff from the MDM server. This should only be used for testing purposes.
- **Allow user to view sent messages** - Shows the messages sent and received via MDM on the user's phone.

Device History Settings

- **Save tracking history** - Allows you to turn tracking history on or off for iOS devices added to the group.

Password Policy



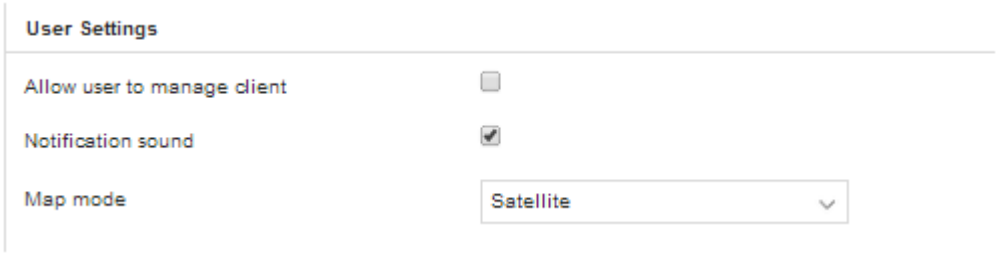
iOS devices offer more control of the password policy compared to Android devices, such as:

- **Minimum number of password characters allowed** - You may select a value from 1-8 or default.
- **Minimum number of complex characters** - Set the number of non-alphanumeric characters allowed in password.
- **Minimum password age** - Set the amount of days a password shall be valid for before requiring alterations (default 0 = not enabled).
- **Auto-lock** - Set the amount of time in minutes, when idle, the device remains active for, before automatically locking.
- **Password history**-How many other passwords you can set before you are able to reuse the same password again.
- **Require Passcode**- Set the amount of time a device may remain locked for before requiring the user to enter the password when unlocking the device.
- **Maximum number of incorrect password entries** - Set the allowed amount of incorrect password attempts, which when exceeded, shall wipe all data on the device.

Location Provider Settings

- **Location update interval -** Specifies the time interval (in minutes) in which the phone will send a location update to the server.
- **Minimum Location Update Distance** - Specifies the minimum distance (in meters) that a device should move from its last recorded position to trigger a location update, also known as Geo-fencing.
- **Send Location Updates** - This setting defines whether or not to send location updates to the server.

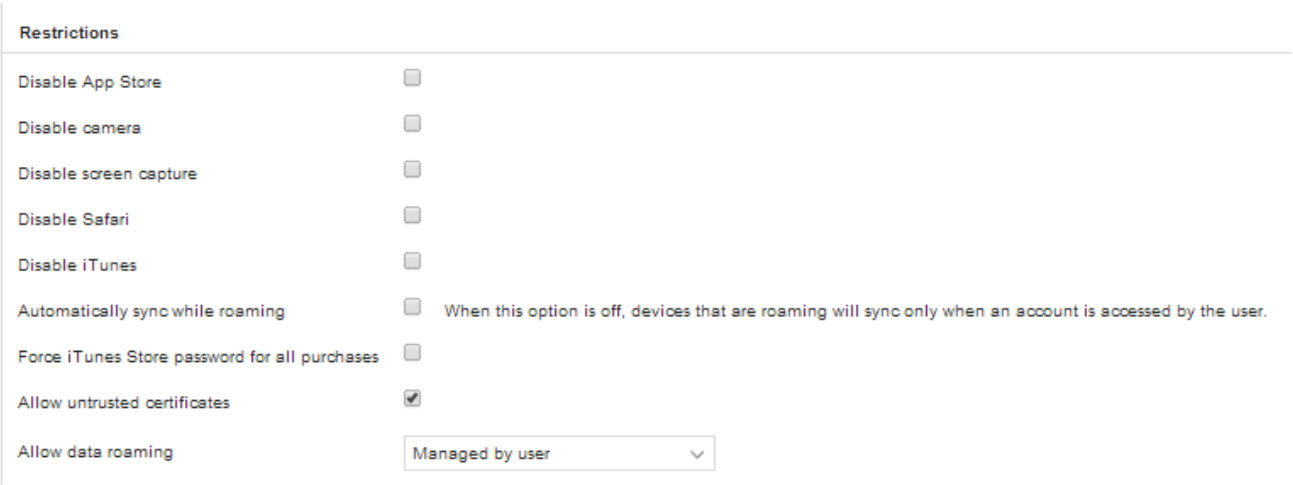
User Settings



User Settings are similar to Android Devices as well:

- **Allow User to Manage Client** - Enables configuration options on the MDM client > Settings, such as:
    - **Advanced** - Allows user to specify MDM Server
    - **Enable tracking** - Allows user to enable or disable position updates
    - **Notification sound**- Allows user to enable or disable sounds when notifications are received
    - **Map Mode** - Allows user to review the MDM client map as satellite, traffic or both.
- **Notification Sound -** A notification sound will be played when a message is received.
- **Map Mode** - When sending directions, this will show either a traffic or a satellite image

Restrictions



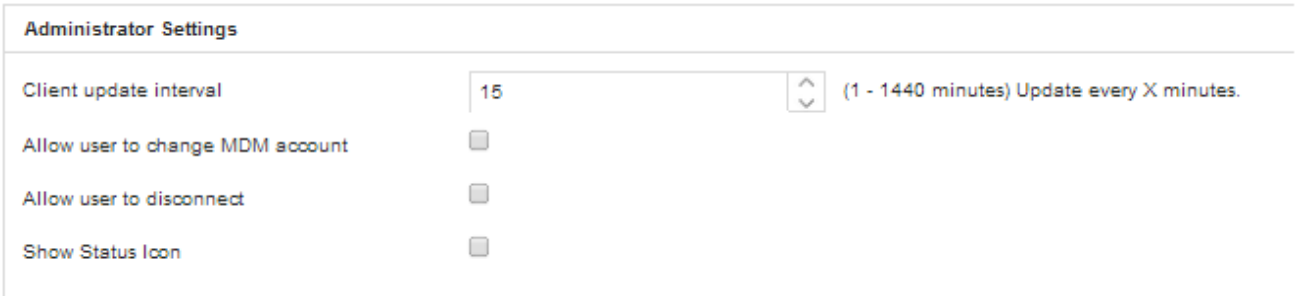
- **Disable the App Store -** Prevents the user from accessing the Apple App Store
- **Disable Camera-** Prevents the user from accessing the camera app on the iPhone
- **Disable screen capture-** Prevents the user from taking screenshots of the iPhone
- **Disable Safari-** Prevents the user from accessing and using the safari browser
- **Disable iTunes-** Prevents the user from accessing and using iTunes
- **Automatically sync while roaming-** Synchronises iOS while the iPhone is roaming
- **Force iTunes password for all purchases-** Forces the use of the iTunes password for all purchases made

- **Allow untrusted certificates-** Allows the installation of untrusted certificates on the iPhone
- **Allow data roaming -** Force enable, disable or allow the device user to control data roaming on the device

Policies for Windows Devices

In the Windows policy tab you can specify the policy settings that will be applied to Windows 7/8 devices.

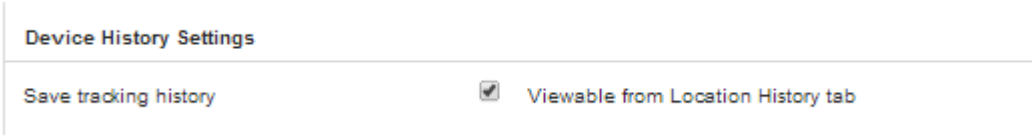
Administrator Settings



The Administrator Settings are somewhat different to the Android and iOS administrator settings

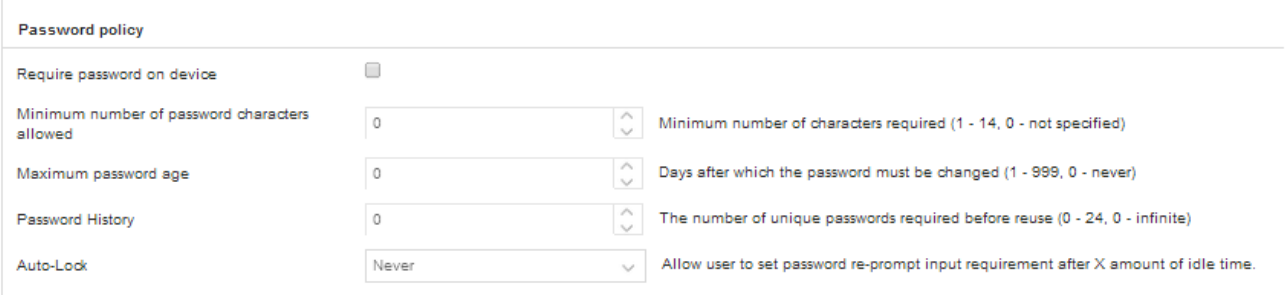
- **Client Update Interval -** This defines the time limit in minutes in which the client will send updates to the server.
- **Allow user to change MDM account** - This option allows a user to logoff and logon to another MDM account. This option is turned off by default and only recommended for testing purposes.
- **Allow user to disconnect** - This allows a user to log off from the MDM server. Should only be used for testing purposes.
- **Show Status icon** - Enables/Disables showing the MDM Status icon on the taskbar.

Device History Settings



- **Save tracking history** - Allows you to turn on or off tracking history for your iOS devices in the group.

Password Policy



Password Settings for Windows devices include:

- **Required Password on Device** - Your device will be required to have a password set.

- **Minimum number of password characters allowed** - This is the minimum number of characters that you can set for a password.
- **Maximum password Age** - Number of days that the password will be valid for before it needs changing.
- **Password history** - How many other passwords you can set before you are able to reuse the same password again.
- **Screen Lock** - The amount of time the device is allowed to remain idle before the screen locks automatically.

Location Provider Settings

- **Minimum Location Update Distance** - Specifies the minimum distance that a device should move to trigger a location update.
- **Send Location Updates** - This setting defines whether or not to send location updates to the server.

Deploying Email and Exchange Accounts

Introduction

With Mobile Device Manager it is possible to configure email and exchange settings for users and push out this configuration to their mobile devices. This will save an administrator a lot of time which would be otherwise wasted explaining to the user how to configure the settings correctly. Furthermore, this function also allows an administrator to quickly delete the corporate email and exchange accounts from the device, without having to remote lock or wipe the device.

Email and exchange configuration is currently supported on both Apple iOS and Android devices.

AquaMail for Mobile Device Manager

Mobile Device Manager can push out email and exchange configurations to iOS and Android devices. In the case of iOS, MDM uses the inbuilt Apple mechanism to configure the apple client on the device. In the case of Android, MDM needs to push out an email client, AquaMail, to be able to control the email configuration from Mobile Device Manager. This is because the stock Android email client does not have remote configuration capabilities.

However, the stock Android Email app is very limited and AquaMail is a much respected email client that has significant capabilities over and above the stock email client. It is also much more user friendly. MDM bundles the AquaMail client at no cost with Mobile Device Manager.

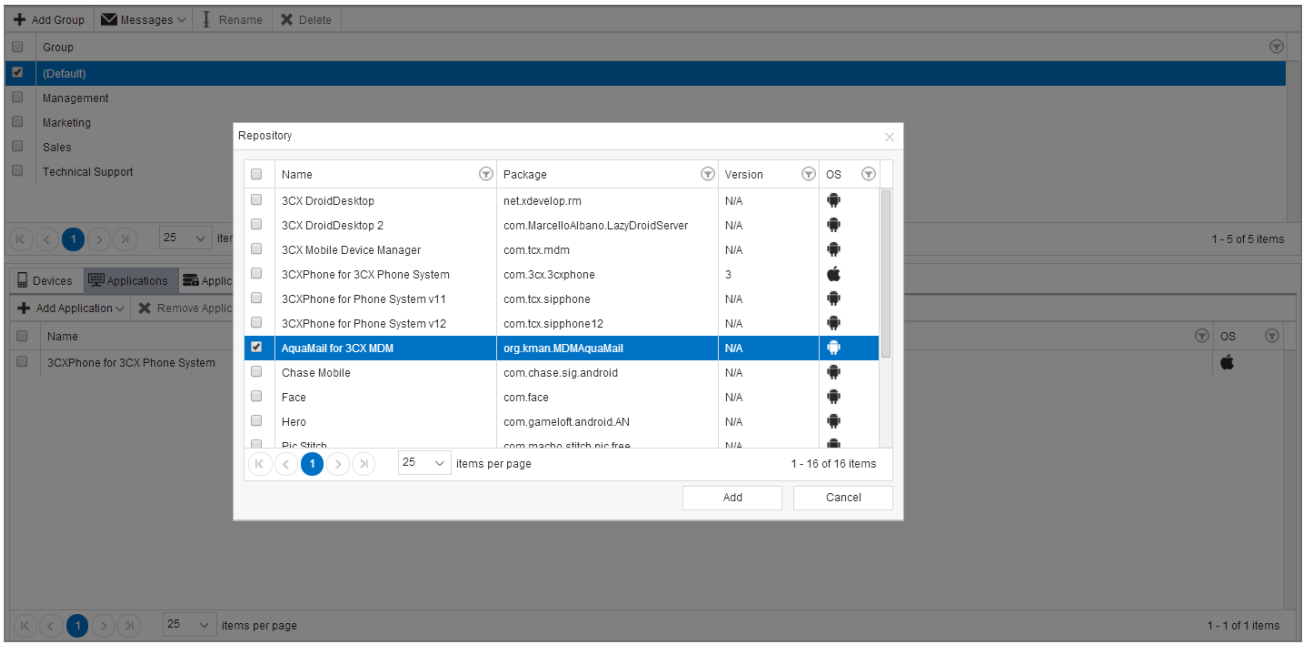
AquaMail Advantages over Stock Android Client

1. Push mail (IMAP IDLE, instant incoming email delivery) for those servers that support it
2. Many mail configuration options including separate notification settings for each account, Night, Silent, Weekend modes and other.
3. Can save attachments on the memory card, can attach any file type, can download compressed files and decompress them automatically for the user.
4. Message autofit (like in Gmail) on Android 4.0 and above.
5. Easy automatic setup for popular email services: Gmail, Yahoo, Hotmail (POP3 only), FastMail, Apple mail services.
6. Exchange accounts pushed through the MDM client app.

Installing AquaMail for MDM on Android Devices

To have AquaMail automatically installed on each new device added to Mobile Device Manager, add it to the default policies node of the Default group, as well as any new groups you create. To do this:

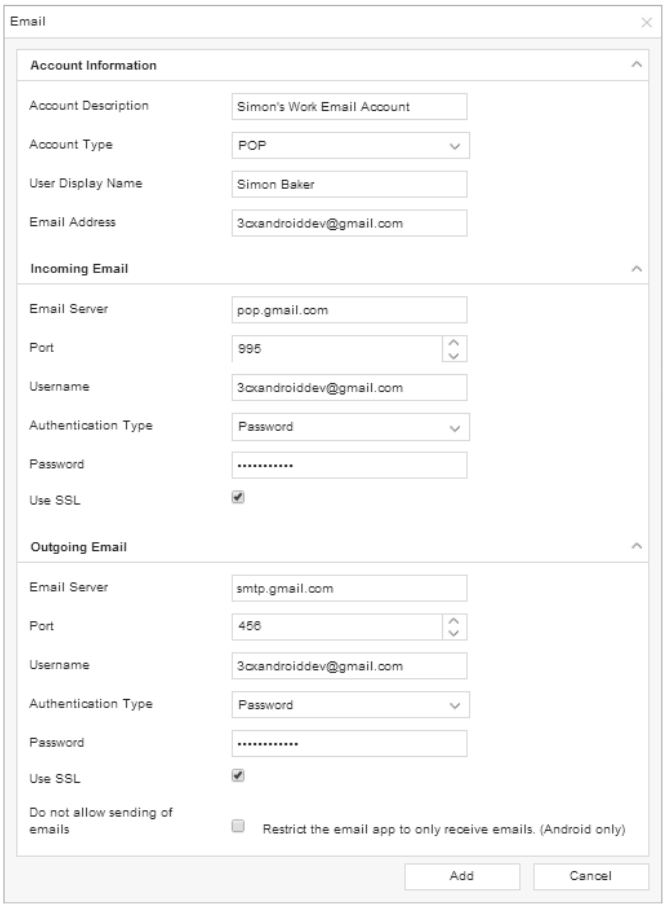
1. Log into the MDM portal using your credentials and click on the ‘Group Policies’ node.
2. Select the Default group (or any other group you may want to install AquaMail on) and click on the ‘Applications’ tab.



3. Select ‘Add Application’ and then ‘From Repository’ (AquaMail is included by default in the MDM App repository for easy access).
4. Find the ‘AquaMail for 3CX MDM’ entry, tick the checkbox and press ‘Add’. This will add the MDM AquaMail app to all the devices that join the Default group (all devices added are initially assigned to the Default group).
5. Accept the deployment and installation of AquaMail for 3CX MDM on your mobile devices.
6. It is now possible to remotely configure the email client on your smartphone.

Adding Email Accounts

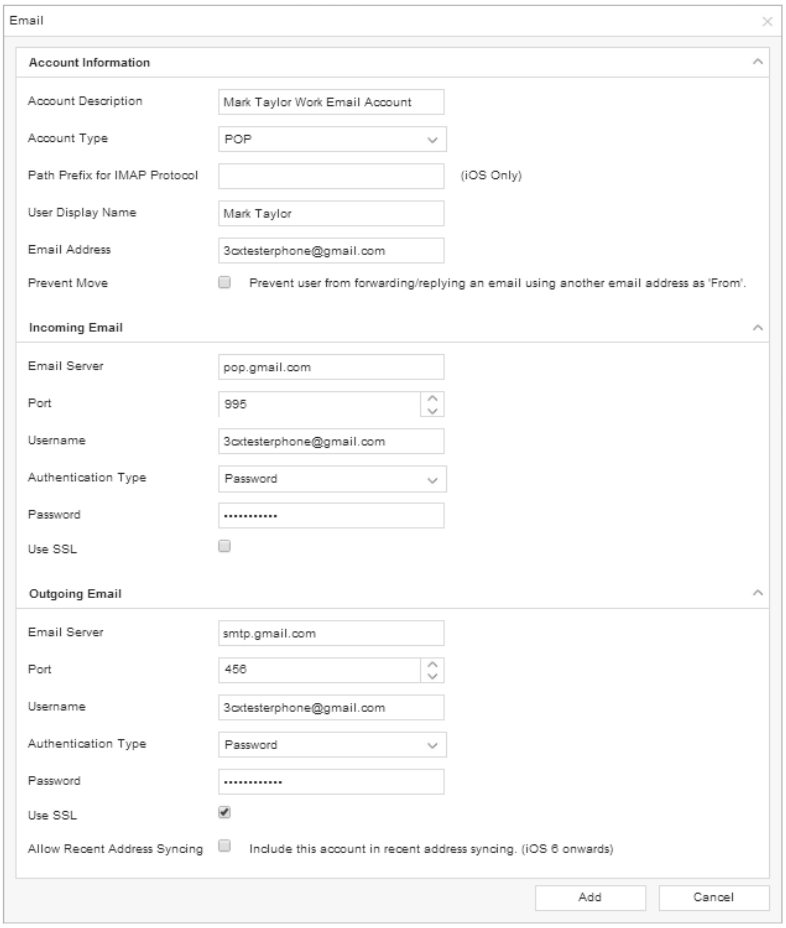
Android



To configure an email account to AquaMail through the MDM app, perform the following steps:

1. Click on the ‘Devices’ node and select the device that the new account is to be pushed out to.
2. Click on the ‘Email’ tab and then click ‘Add Account’.
3. Fill in the account details such as the account description, account type, email address and configure the incoming email and outgoing email server settings. These settings are dependent on who is your email provider. In the above example a Gmail account was used. Note that your email provider settings might vary.
4. Once you finish filling out the email account settings, click ‘Add’. The email profile will now be pushed out within a few seconds to the AquaMail client on your device and AquaMail will configure the email account automatically.

iOS

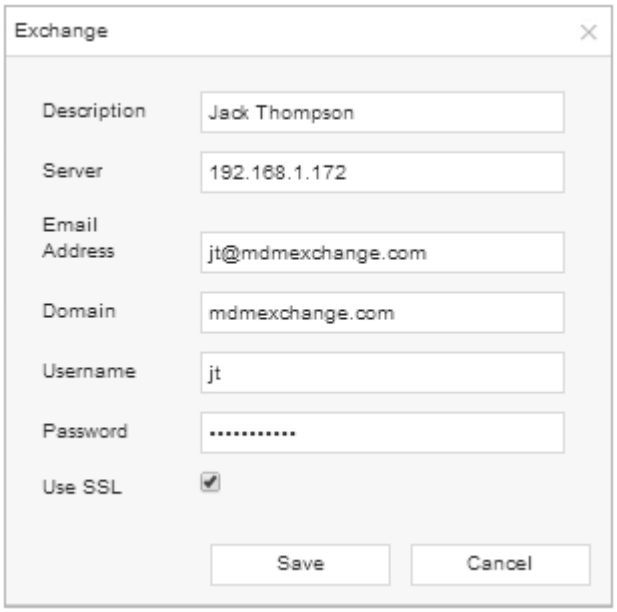


To configure and push an email account to the mail client through the MDM app for an iOS based device please follow the next steps:

1. Click on the ‘Devices’ node and select the iOS device that you want to deploy the new email account on.
2. Click on the ‘Email’ tab and then press ‘Add Account’
3. Fill in the account details such as the account description, account type, email address and configure the incoming email and outgoing email server settings. These settings are dependent on who is your email provider. In the above example a Gmail account was used, so your settings might vary.
4. Once you finish filling out the email account settings, click ‘Add’, The email profile will now be pushed out to your iOS device.

Adding Exchange Accounts

Android

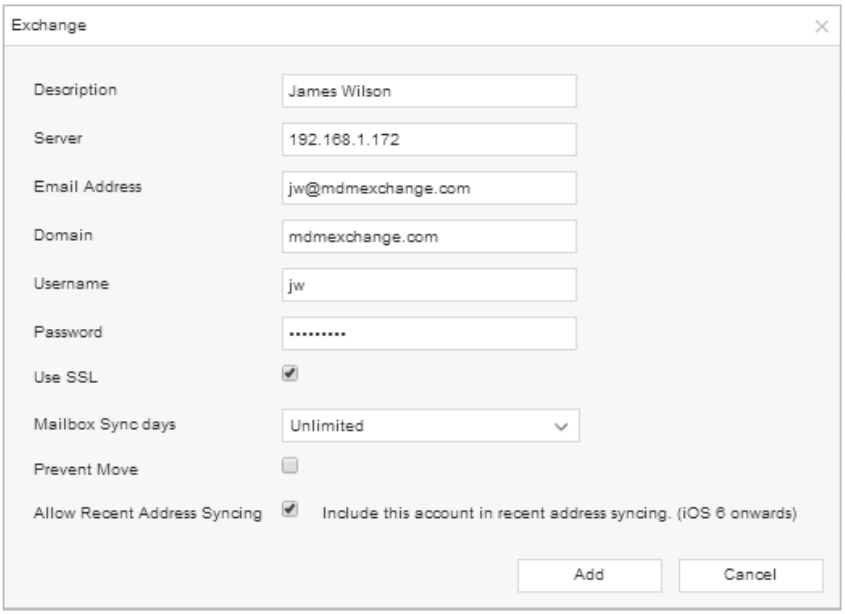


To configure and push an Exchange account to the AquaMail for 3CX MDM app for Android based devices please follow the next steps:

1. Click on the ‘Devices’ node and select the device that you want to deploy the new email account on.
2. Click on the ‘Exchange’ tab and then press ‘Add Account’
3. Next, fill in the below details:
    - Description - Add a description regarding this account
    - Server - Enter the Exchange server IP/ FQDN.
    - Email Address - Enter the email address of the mailbox/ account being configured
    - Domain - Enter the Exchange server domain
    - Username, Password - Enter the Exchange account username and password
    - SSL - Enable if SSL is required by Exchange
4. Once you finish filling out the exchange account settings, click ‘Add’, The email profile will now be pushed out to your Android device.

Note: AquaMail client is required. If this has not already been installed, upon clicking add, the MDM client shall notify the device user.

iOS



To configure and push an Exchange account to the iOS mail client through the MDM app for an iOS based device please follow the next steps:

1. Click on the ‘Devices’ node and select the device that you want to deploy the new email account on.
2. Click on the ‘Exchange’ tab and then press ‘Add Account’
3. Next, fill in the below details:
    - Description - Add a description regarding this account, taking the above screenshot as an example.
    - Server - Enter the Exchange server IP/ FQDN.
    - Email Address - Enter the email address of the mailbox/ account being configured.
    - Domain - Enter the Exchange server domain.
    - Username, Password - Enter the Exchange account username and password
    - SSL - Enable if SSL is required by Exchange
    - Mailbox sync days - Select the frequency which you require the mailbox to sync with the Exchange account.
    - Prevent Move - If enabled, messages may not be moved out of this exchange account and into another. In addition, this also prevents forwarding or replying from a different account than the message originated from.
    - Allow Recent Address Syncing - When enabled, this account is excluded from address recent syncing.

Deleting Email/ Exchange Accounts

With AquaMail for 3CX Mobile Device Manager it is possible to delete email/ Exchange accounts individually. This is very useful as the user might have configured a personal email/ Exchange account and would like to keep his personal email. AquaMail has many advantages over the stock android email client.

When you delete an email/ Exchange account, all account details, the email AND THE ATTACHMENTS are wiped from the device instantly, ensuring that no confidential information is left behind.

To delete an Email account:

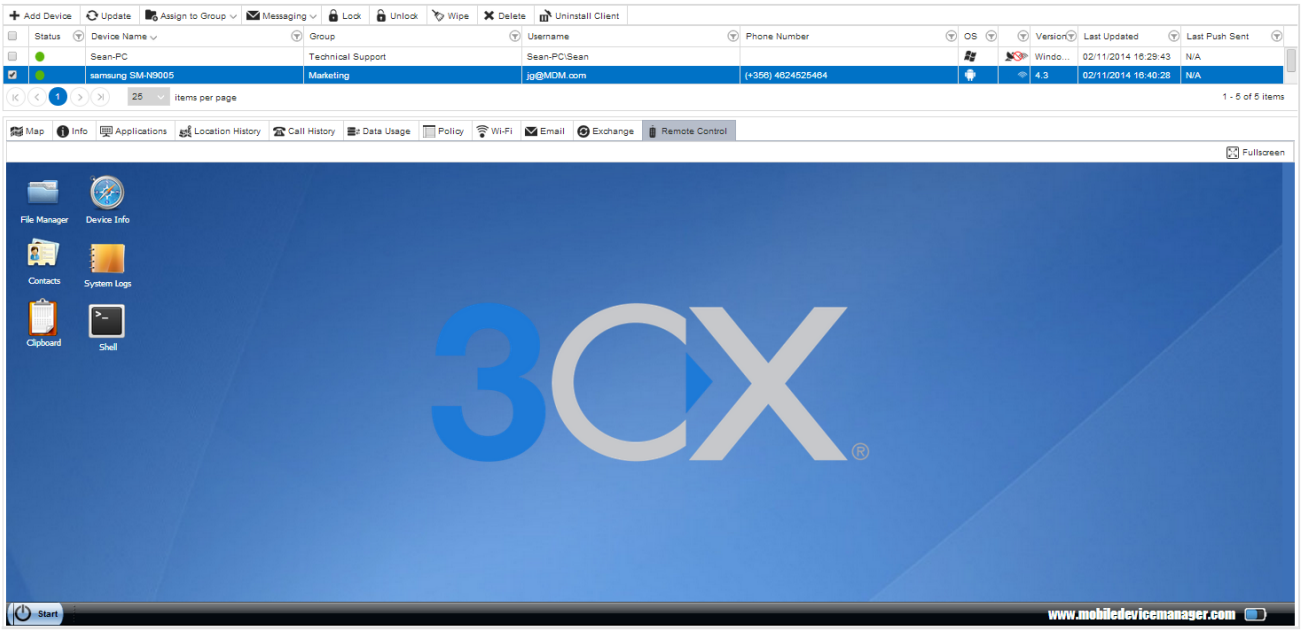
1. Go to the ‘Devices’ node and select the device which you want to delete the email account from.
2. Click the ‘Email’ tab and you will be taken to the email account list.
3. Enable the checkbox next to the account that you want to delete and click the ‘Delete’ button.
4. Click OK to confirm the deletion at the next dialog that will appear.
5. The account will be removed both from the AquaMail client on your android device and from the email tab in the MDM administration console.

To delete an Exchange account:

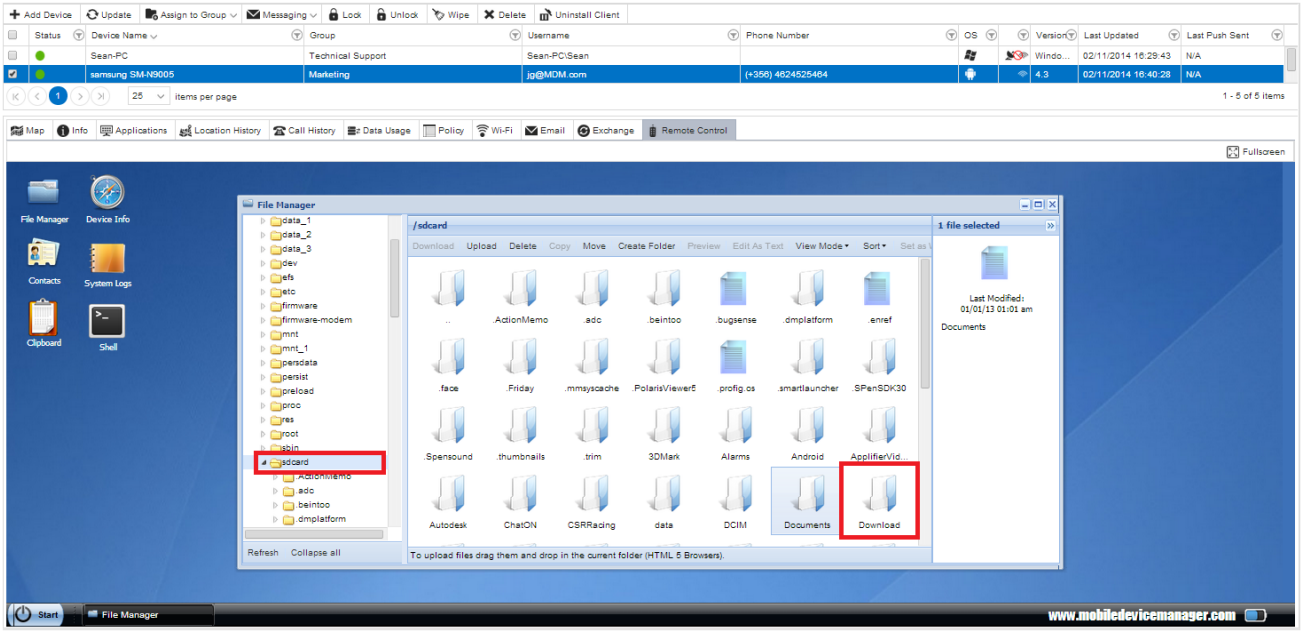
1. Go to the ‘Devices’ node and select the device which you want to delete the Exchange account from.
2. Click the ‘Exchange’ tab and you will be taken to the Exchange account list.
3. Enable the checkbox next to the account that you want to delete and click the ‘Delete’ button.
4. Click OK to confirm the deletion at the next dialog that will appear.
5. The account will be removed both from the AquaMail client on your android device and from the Exchange tab in the MDM administration console.

Deleting Files from the Attachment Directory

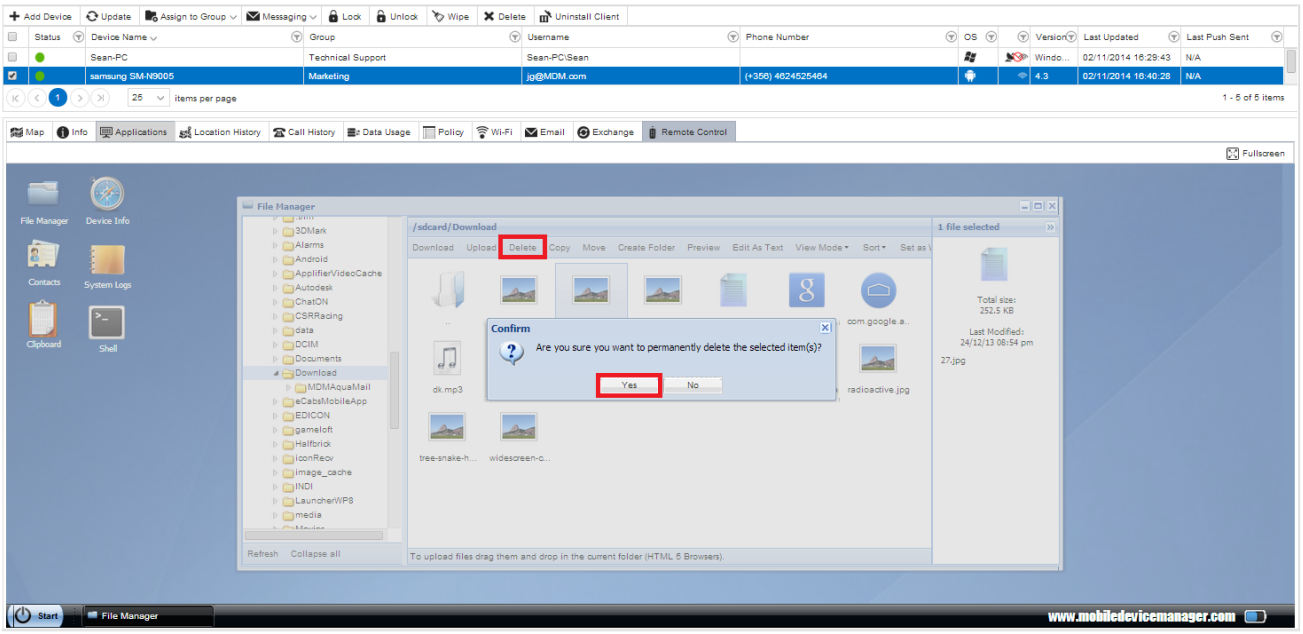
To delete attachments from your email account's attachment directory selectively without removing the account please follow this procedure:



1. Select the device that you want to delete attachments from the 'Devices' node and click on the 'Remote Control' tab. The remote control tab will open up and load in the MDM portal window.



2. Click on 'File Manager' on the window to start the file manager and browse to your attachment folder (Prior to searching for the attachment folder, check the AquaMail client settings, default is 'Download'). Double click to open it.



3. Select the attachments that you want to delete and press the ‘Delete’ button in the File Manager. Confirm the deletion by selecting ‘Yes’ at the dialog that appears. The selected files will be deleted from your attachment folder.

Location Tracking

Introduction

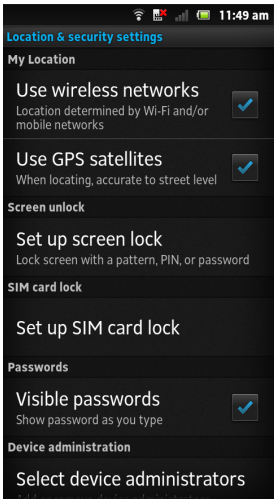
The location tracking feature allows you to know the exact whereabouts of all your mobile devices. This information is reported in real time in Mobile Device Manager, and recorded so that you can create detailed location history reports.

Requirements

Location is resolved on the phone and then sent to the MDM platform. Therefore the phone must be able to send the location to MDM via GPS or Network (Wi-Fi/3G).

Android Devices

The MDM client will send location updates every 15 minutes by default OR whenever the devices moves a specified minimum distance(Geo-fence (meters) set from Devices> *select device*> Minimum location update distance). To be able to do this it needs permission from the Android phone to do tracking. Tracking by Network or GPS needs to be switched on to report location.



These settings are found in the Location & Security settings (Android 2.3) or Location Services (Android 4.0.3 and above). The MDM client will prompt the user to switch on tracking by Network or GPS if you 'enforce' tracking.

iOS Devices

The main function of the iOS MDM client is Location Tracking. Other MDM features are performed without the need for a client. To be able to perform location tracking, the client must be installed and active.

Note that if an Apple iPhone is rebooted, the MDM Agent is not automatically started. The administrator can push a message to the user to confirm starting of the MDM Agent, but the process cannot be performed silently due to Policy Restrictions on the Apple phones themselves.

Network or GPS Location Tracking

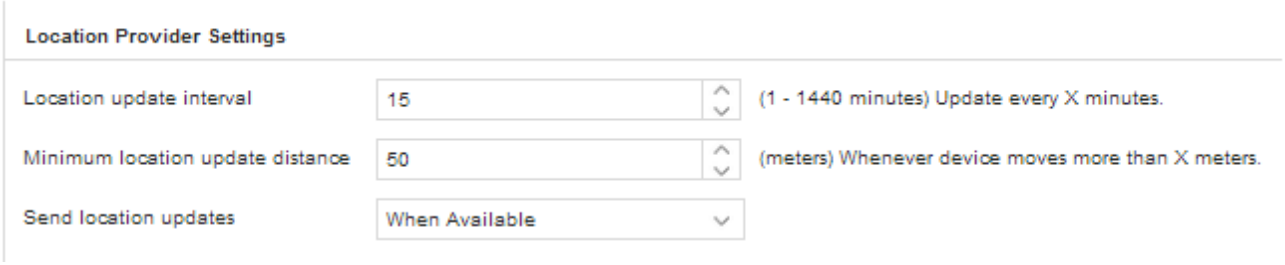
As an administrator you can decide whether location should be tracked by Network, by GPS or both. GPS is more accurate, but switching on the GPS on the phone will cause the phone to use more battery power. At the same time, GPS Location Tracking will not work well within a building. Network Location Tracking is relatively accurate, and requires little battery power.

Checking that the Phone has Location Tracking Enabled

GPS Tracking	Disabled
Network Tracking	Enabled

You can check whether the phone has Network tracking or GPS enabled by going to the Device > Info tab.

Location Settings



Location Tracking options are available per device or per group of devices. To configure Location Tracking Settings, select the device or group of devices and go to the Policy Tab. Scroll down to the Location Settings group.

The following Location Tracking settings are available:

Location Update Interval and Minimum Location Update Distance

The location update interval specifies the time interval (in minutes) that the phone will send a location update to the server, even if its position has not changed.

The Minimum Location Update Distance setting specifies the minimum distance that a device should move to trigger a location update. Location updates are sent to the server whenever the mobile devices change position. You can configure the distance that should trigger a location update here. By default, a location update is triggered if the device moves by more than 50 meters.

Save Tracking History

This option allows you to enable or disable storing of the location history. When this option is enabled the location history of the device will be saved, either when the location update interval expires or the device moves more than the minimum location update distance. You have the option of deleting the location history by selecting a device then going to the Location History tab and deleting the tracking history.

Send Location Updates

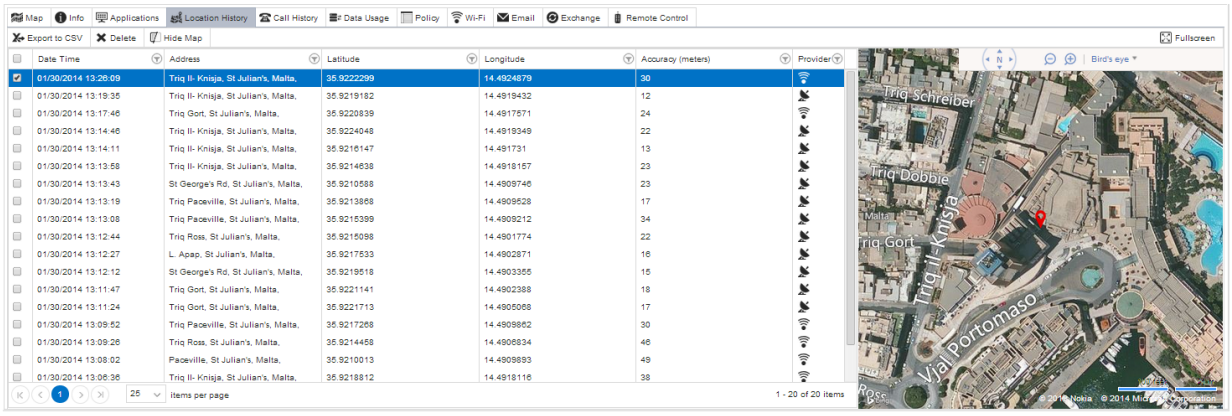
This setting defines how location updates are collected and sent to the server. The following options are available:

- Force Network only - This option attempts to send location updates via Network only and will alert the administrator and user if the phone is not configured to allow sending of updates.
- Force GPS / Network - This option attempts to send location updates via GPS OR Network, and if neither is available sends an alert to the administrator and prompts the user to enable location tracking.
- Force GPS only - This option will attempt to send location updates via GPS only and if GPS is switched off the user and the administrator will be alerted.
- When Available - This will send location updates only if the phone is configured to allow it. It will not prompt the administrator or the user if no location updates can be sent. For example if a user switches off location tracking entirely from his phone, the administrator nor the user

will be notified.
- Off - Turns off location tracking

Since Geolocation privacy laws are not clearly defined in many countries around the world or you do not want to track the company devices after working hours, you now have the option to turn location tracking completely off. That makes sure that no location tracking data will be collected if you are using MDM in a country that demands explicit Geolocation permissions and that you are in no danger of violating private data laws in areas that this is forbidden.

Location History Tab



To view the location history of a device, click on the device and select the Location History tab. The date, address, Latitude, Longitude and accuracy will be shown. In addition, the icon will show how the location was obtained being either via GPS or via Wi-Fi.

Filtering Location History

You can filter the Location History by date, address, latitude, longitude, accuracy and provider. To do this, click on the funnel symbol located to the right of the respective information column.

Exporting Location History

You can export Location History into a CSV file for further analysis in another application such as Microsoft Excel.

Delete Location History

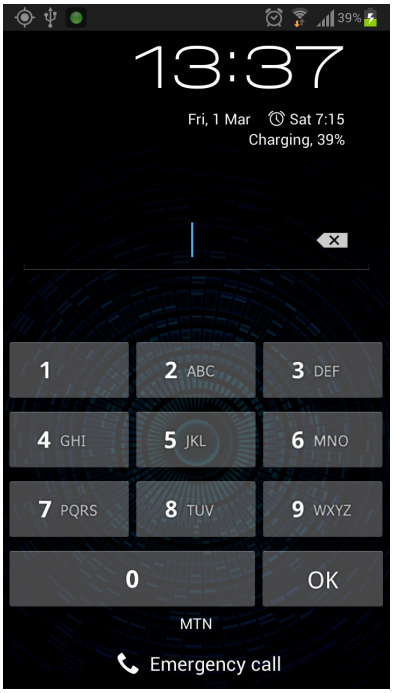
You also have the option of deleting Location History. To do this click on the Location History entry that you want to delete and press the delete button and confirm.

Security Features

Introduction

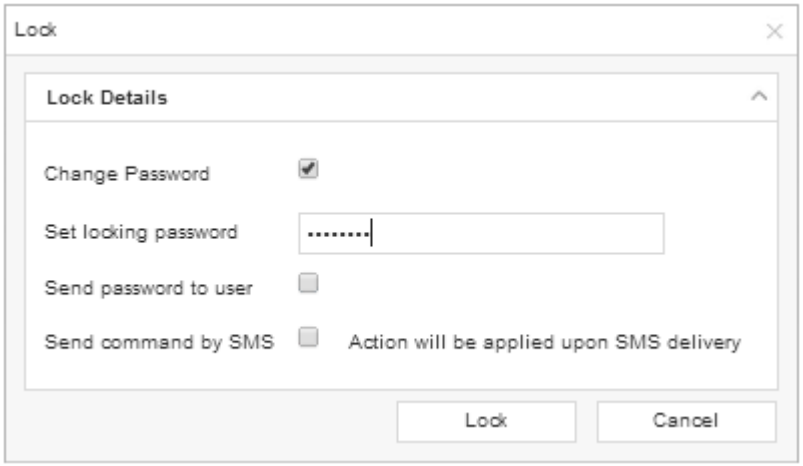
Mobile Device Manager allows you to secure your mobile devices by enabling you to enforce Password Policies, Remote Lock and Remote Wipe mobile devices.

Remote Lock



With the Remote Lock feature, you can easily lock a phone that you suspect might be lost or is being misused. This will automatically lock the phone and present the PIN entry screen to the user.

Note: On iOS you can force a Lock, but not specify the password. The existing password configured on the device will be used.



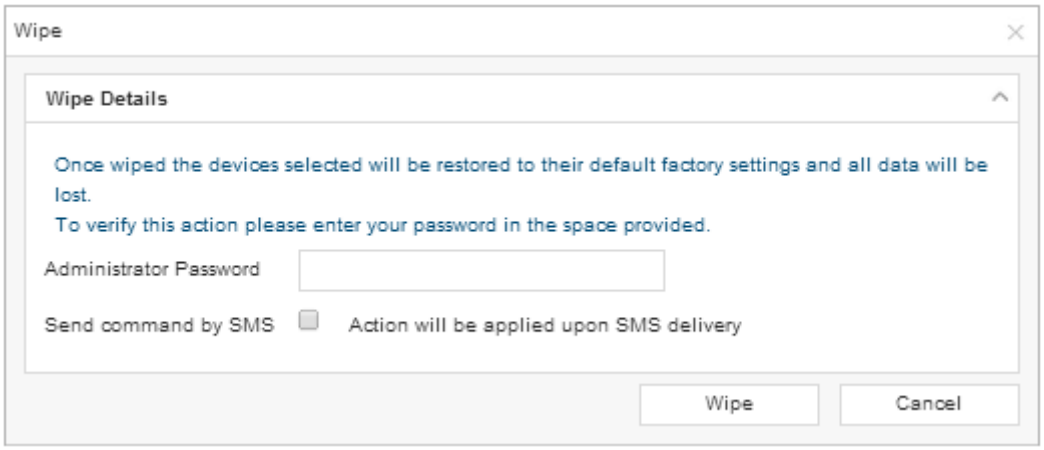
To Remote Lock a device:

1. From the devices node, select the device to be locked.
2. Click on the ‘Lock’ button.
3. Enter the PIN that you wish to set.
4. Decide whether you want to send the PIN to the user.
5. Decide whether you wish to send the command by SMS as well, to ensure that the Remote Lock is performed even if there is no data connection available.

6. The phone will be locked and will require the password to unlock.

Remote Wipe

If the device has been lost, it is best to wipe all the data and the configuration off the device using the Remote Wipe feature. When triggering the Remote Wipe feature, an SMS is sent to ensure that the remote Wipe takes place as soon as possible. This way, even if the device is not connected to the data network, the remote wipe is still done immediately. The device is returned to the factory default settings, and the SD card is wiped as well.

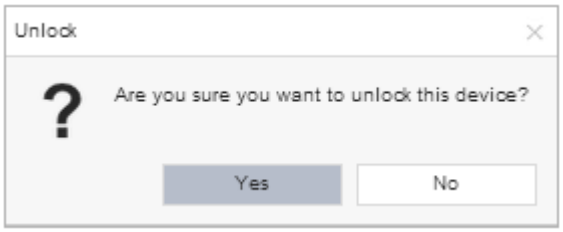


To Remote Wipe a device

1. From the 'Devices' node, select the device to be wiped.
2. Click on the 'Wipe' button.
3. Enter the administrator password for additional security.
4. Decide whether you wish to send the command by SMS as well, to ensure that the Wipe is performed even if there is no data connection available.
5. The phone will be wiped and reset to factory default.

Remote Unlock

If the device has been found or has been locked by accident and you do not remember the password that you used to lock the device you can now use the 'Remote Unlock' feature to unlock it.



To Remote Unlock a device:

1. From the 'Devices' node select the device to be unlocked
2. Click on the 'Unlock' button
3. Select 'Yes' at the prompt, a confirmation message will appear and your device will be unlocked

Password Policy

With MDM you can enforce a strong device password policy across all their mobile devices and set the minimum password length, time lapse before a device auto-locks and the maximum number of failed password. This is a basic security feature that will greatly enhance the security of mobile devices. If the device is lost, it will allow you enough time to remote wipe the device.

To enforce a Password Policy:

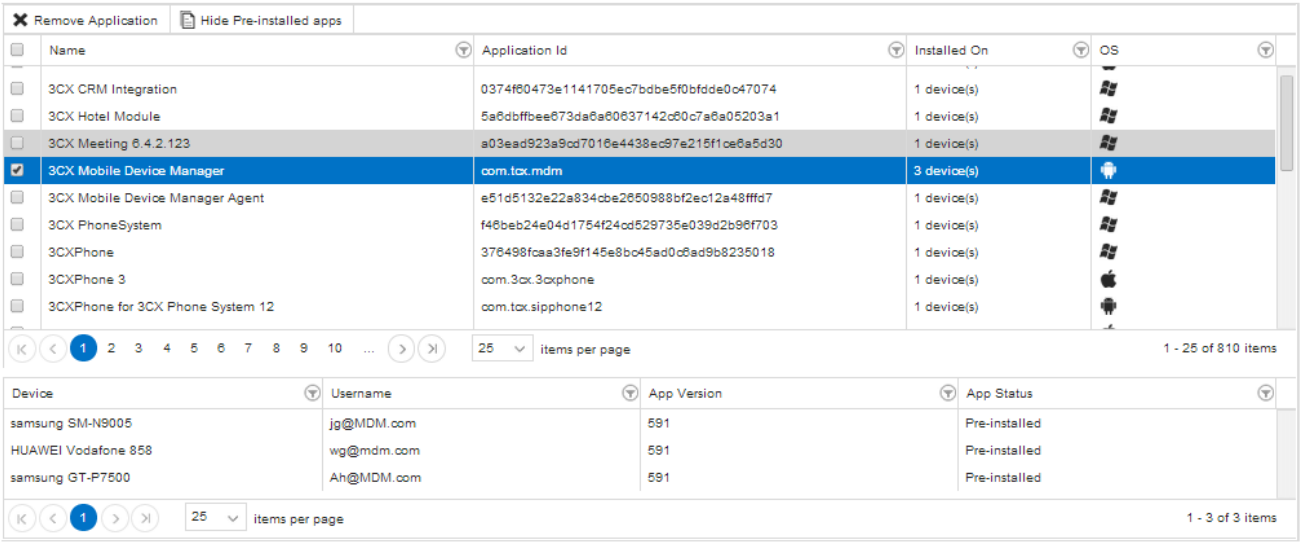
- Select the device in the devices node and go to the Policy tab.
- Or Select the Group policy and go to the Android or iOS Policy tab.
- Android: Alter the Password Policy setting in the Password Settings section. Select:
    - No password policy enforced
    - Password required (Any)
    - At least a numeric password required
    - At least an alphabetic password required
    - An alphanumeric password required
- iOS: Alter the Password Policy as required. iOS has many more Password Policy options, all shown in the interface of MDM.

Monitor for Malware

It's important to regularly monitor installed apps for potential malware or adware. With Mobile Device Manager administrators can review all applications that are installed on all the devices from a single screen and remove unsafe apps with a mouse click.

Google Play will -from time to time- issue alerts about unsafe apps, often distributed by app stores not operated by google, but administrators do not have an easy way of finding these apps on a large number of devices. Mobile Device Manager allows you to view potential 'bad apps' and uninstall them.

To view all installed apps on all mobile devices, go to the App Management node and then to the 'Installed Apps' node.



Application Management

Introduction

Mobile Device Manager allows you to manage applications installed on your mobile devices. You can review installed applications on each mobile device, push out applications onto the phone, as well as de-install applications with a few mouse clicks. Application management can be done for an individual device, for a group of devices or for ALL mobile devices managed by you.

Deploying Apps

You can deploy apps to individual mobile devices or to groups of mobile devices;

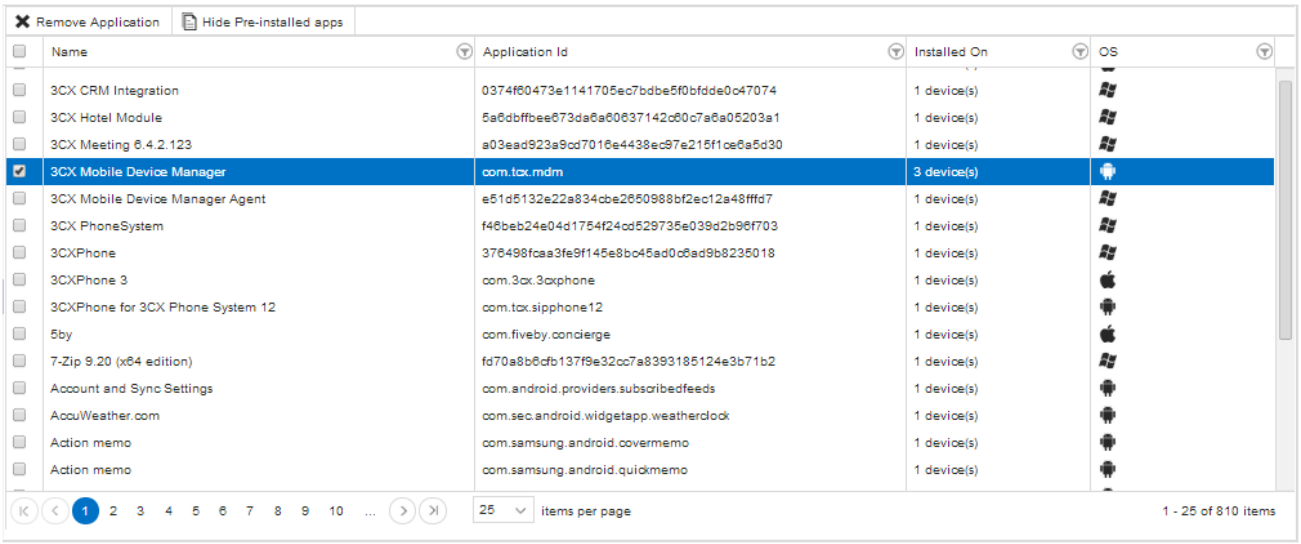
1. To deploy an app to a single mobile phone, select the device and go to the 'Applications' tab.
2. To deploy an app to a group of mobile devices, go to the 'Group Policies' node, select the group and go to the 'Applications' tab.
3. Now select the App from Google Play, the Apple App Store, Add from Repository or select the actual application file (APK).

Removing Apps

You can remove apps from individual mobile devices or groups of devices as follows;

1. To remove an app from a single mobile phone, select the device and go to the 'Applications' tab.
2. To remove an app from a group of mobile devices, go to the 'Group Policies' node, select the group and go to the 'Applications' tab.
3. Click 'Remove Application' to have the application removed.

App Repository



The App Repository allows you to create a repository of enterprise apps that you can easily deploy to one or more mobile devices. You can refer to the App Repository from the 'App Management' Group, from the phone's 'Applications' tab or from the 'Group Policies' Applications tab.

Application Control

Mobile Device Manager allows you to proactively control what apps get installed to any mobile device. This is achieved via Whitelisting or Blacklisting apps. These functions are mutually exclusive, i.e. you must either decide to take the Whitelisting approach or the Blacklisting approach.

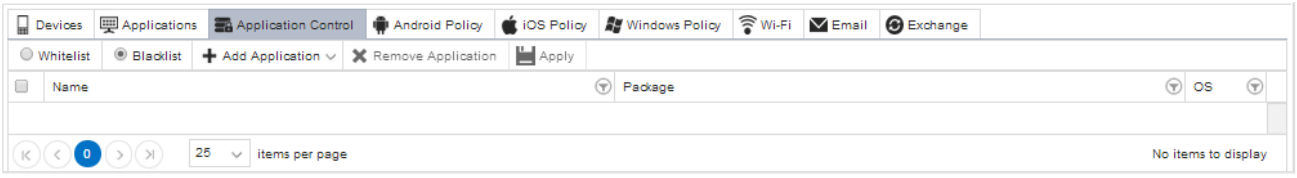
Whitelisting Apps

This function will allow users to install only those apps that are listed in the Whitelist. You will need to list all apps that may be installed on the devices.

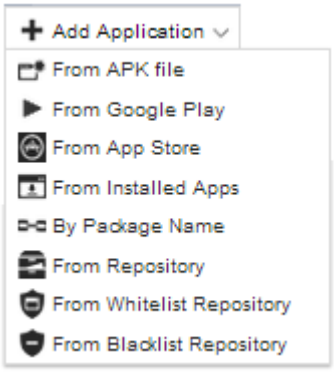
Blacklisting Apps

This function will block users from installing apps that you list as Blacklisted. To create a Blacklisted or Whitelisted app:

1. Select the Group Policy for which you want to Whitelist or Blacklist an app.
2. Go to the 'Application Control' Tab.



3. Specify the whether the App will be Blacklisted or Whitelisted
4. Click ‘Add Application’.



5. Add the app in question from one of the above options.

The 'Application Control tab' currently only lists Whitelisted or Blacklisted apps. Currently apps can only be Whitelisted or Blacklisted at Group Policy Level. It is not possible to Blacklist an app system wide or per phone.

Caution: Enabling the ‘Whitelist’ radio button without applications added to the list will not allow ANY applications to be installed on devices added to that group without creating an application control violation.

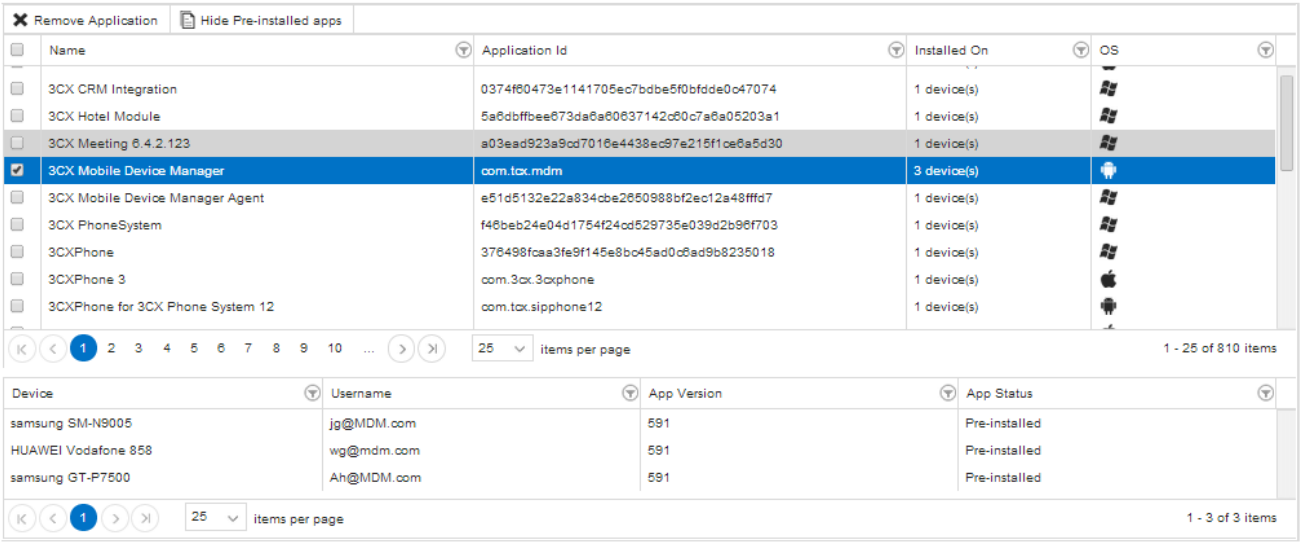
Application Policies

Adding applications will automatically deploy these applications to all devices in the group. You can add applications from the following sources:

- An APK file - directly upload the APK file (Android)
- Google Play - will install the app from the Google Play store
- Appstore - will install the app from the Apple App Store
- Repository - You can install apps stored in the App Repository

NOTE: If you wish to configure email on android devices for users, you must ensure that the AquaMail for 3CX MDM app is deployed.

Viewing Apps Installed on All Mobile Devices



Reviewing apps installed on all devices on a regular basis helps ensure that no malware or inappropriate apps are present on mobile devices that you manage.

To see all the applications installed on all mobile devices go to the 'App Management' group and then click on the ‘Installed Apps’ node. This shows all the applications installed on all mobile devices. You can see the application Name, Application id, how many devices it is installed on and for which OS. In the details tab that appears at the bottom you can see the Device name that the application is installed on, the username associated with that device, the app Version name, and the App Status

Remove one or more applications from ALL devices by selecting the application and clicking 'Remove Application'.

Managing Wi-Fi Settings

Introduction

With Mobile Device Manager it is possible to configure Wi-Fi networks for your users and automatically push out these settings out to the devices.

Secure your Wi-Fi Network

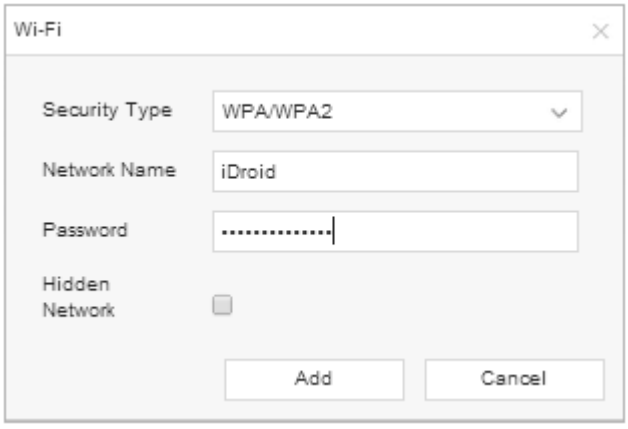
The most important commodity a company has is its data. Most companies today run the risk of losing data or having their data accessed by unauthorised users by disclosing the access password to employees which in turn by accident or oversight reveal it to others. Mobile Device Manager corrects that oversight by pushing the network configuration onto the user's device without revealing the network password.

For companies that adopt the BYOD (Bring Your Own Device) scheme, security is even more paramount since users might use these devices outside the company's secure network thus exposing themselves to greater risks. Companies have had data and funds stolen because old devices used at work were not cleared of their network access rights or because someone had connected to rogue access Wi-Fi point and had their credentials stolen and used afterwards. Using the MDM allows you to see all the networks that a user has connected to and duplicate networks will be spotted easily indicating an attempt from someone to intercept data not send in a secure form.

With Mobile Device Manager you can edit and delete unused Wi-Fi networks and identify Rogue Wi-Fi points. This greatly simplifies the process of Wi-Fi management in a company and allows you to regularly change the Wi-Fi Network passwords as well as remove access to your Wi-Fi network for employees that have left the company and reducing the odds of an unwanted security breach.

Managing Wi-Fi Networks

Adding a Wi-Fi Network



From a selected device within the 'Devices' node, using the Wi-Fi tab you can push out new Wi-Fi Networks to the group of Devices. To specify a Wi-Fi network for a device:

1. Select the device that you want to push your Wi-Fi settings on from the 'Devices' node.
2. Click on the 'Wi-Fi' tab.
3. Click 'Add Network'.
4. Fill in the Wi-Fi network details:

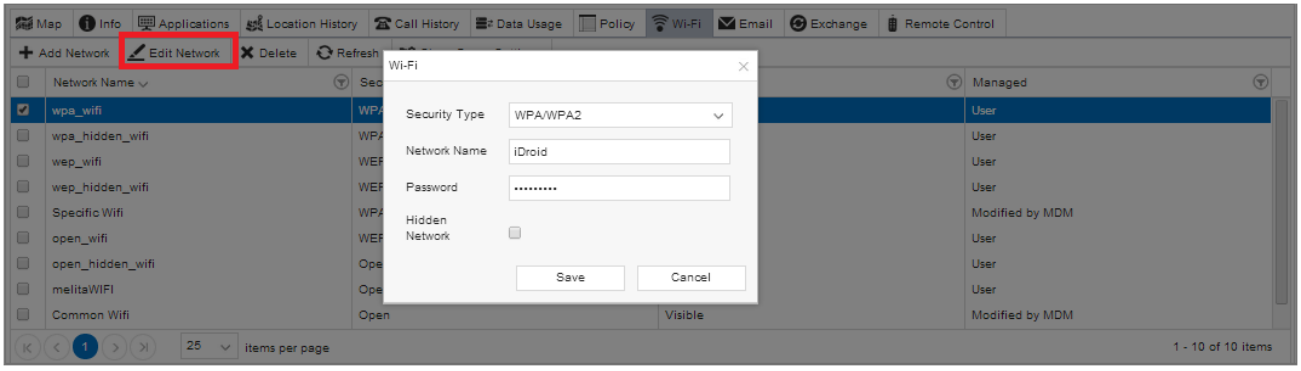
5. **Security Type**: Wi-Fi Protected Access (WPA), Wired Equivalent Privacy (WEP), or Open (no security).
6. **Network Name**: Your Wi-Fi SSID.
7. **Password**: Password to log in to your Wi-Fi network.
8. Whether the network is hidden or not.

After you select your settings press 'Add' to push the Wi-Fi settings to your mobile device.

Editing a Wi-Fi Network

If you want to edit and change the configuration of a Wi-Fi network on a device then:

1. Select the ‘Devices’ node.
2. Click on the ‘Wi-Fi’ tab and select the network that you want to edit.

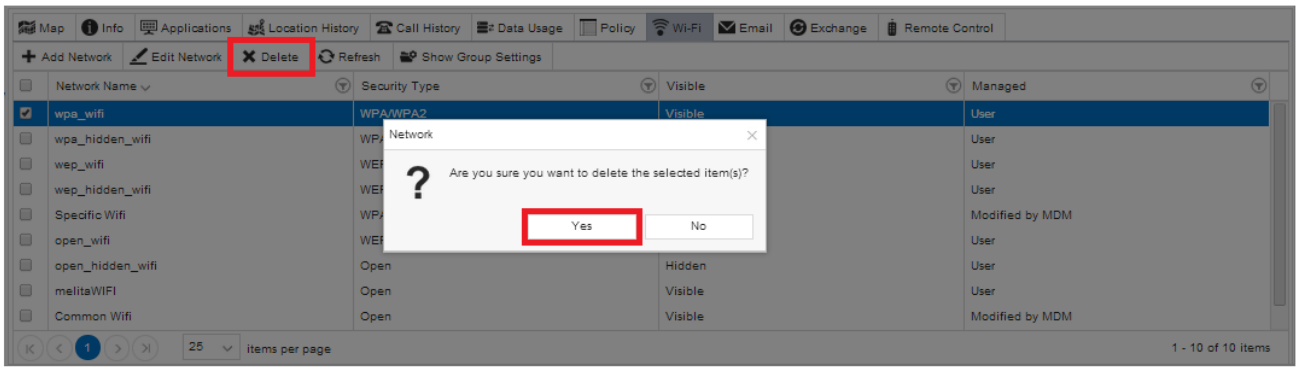


3. Click the ‘Edit Network’ button and make your changes.
4. Press ‘Save’ to save your configuration.

Deleting Wi-Fi Networks

If an employee leaves the company it is important to remove access to the company Wi-Fi network! To remove the Wi-Fi configuration from a User’s device:

1. Select the device that of which you want to remove the Wi-Fi network from the ‘Devices’ node.
2. Click on the ‘Wi-Fi’ tab.



3. Scroll through the network list and select the Wi-Fi network that you want to delete from the device. Click on ‘Delete’.
4. Confirm whether you want to delete the network in the dialog that appears. Press ‘Yes’ to confirm.

Managing Wi-Fi Networks using Group Policies

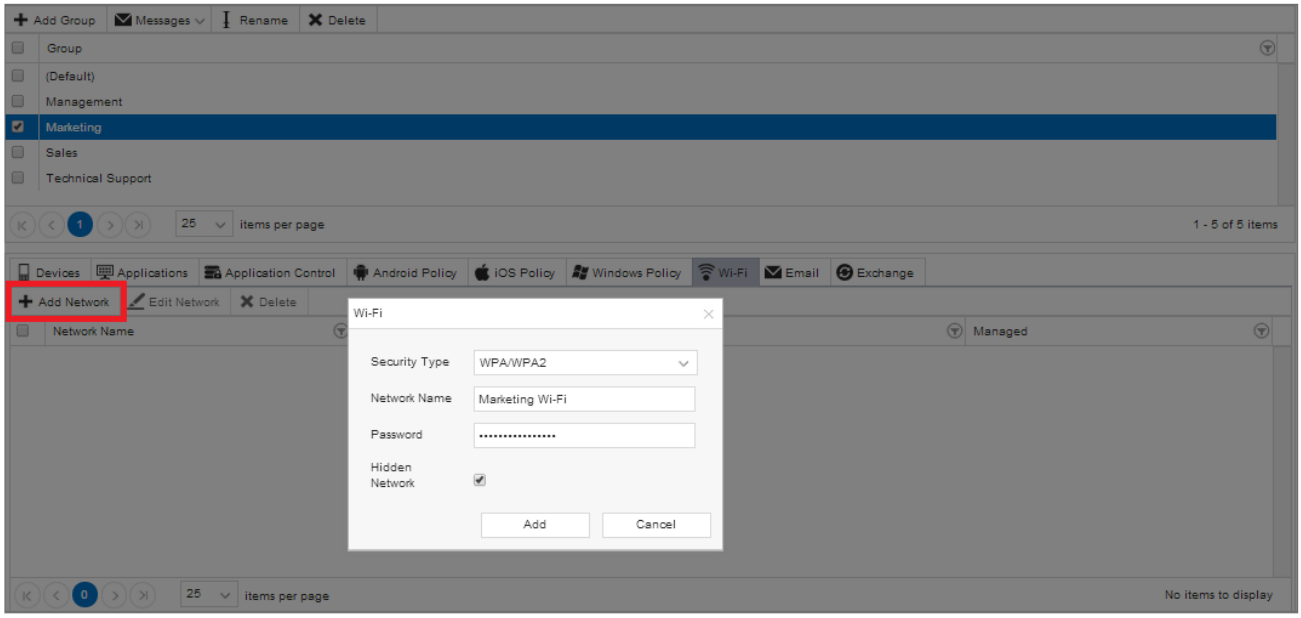
MDM is also able to manage Wi-Fi networks by using Group Policies. This makes it easy to deploy Wi-Fi configurations to multiple devices at the same time as well as editing and removing them simultaneously if the need arises. If for example you decide to change the password for the company Wi-Fi network you now can edit and configure the Wi-Fi settings of the company policy to reflect and deploy the change on all the group devices instead of doing for every device one by one

from the ‘Devices’ node.

Adding a Wi-Fi Network to Multiple Devices

To add a Wi-Fi network to a device group:

1. Click on Group Policies.
2. Select the group that you want to deploy the Wi-Fi configuration on and click on the ‘Wi-Fi’ tab.

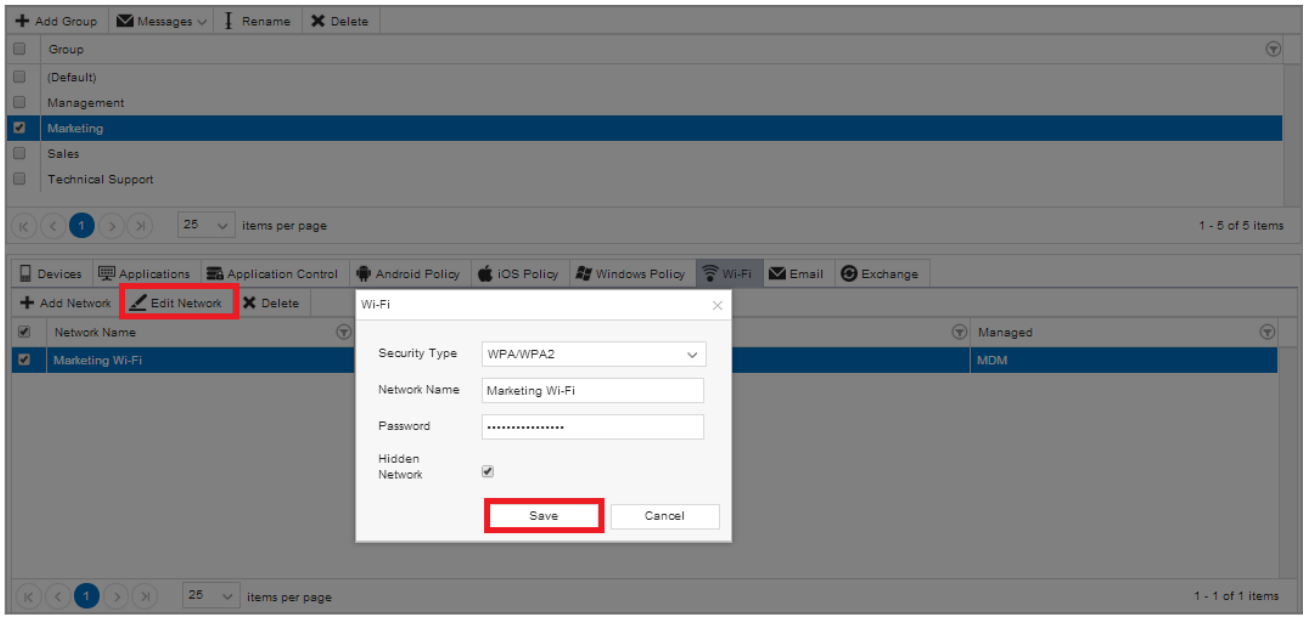


3. Press ‘Add Network’ and fill in the network details (Security type, Network Name, Password and whether it is a hidden network or not).
4. Press ‘Add’ to push out the configuration to your devices.
5. Press ‘OK’ after the confirmation message appears.

Editing a Wi-Fi Network for Multiple Devices

To edit a Wi-Fi Network for a group:

1. Select the ‘Group’ Policies tab
2. Select the group of devices that you want to edit the Wi-Fi configuration.

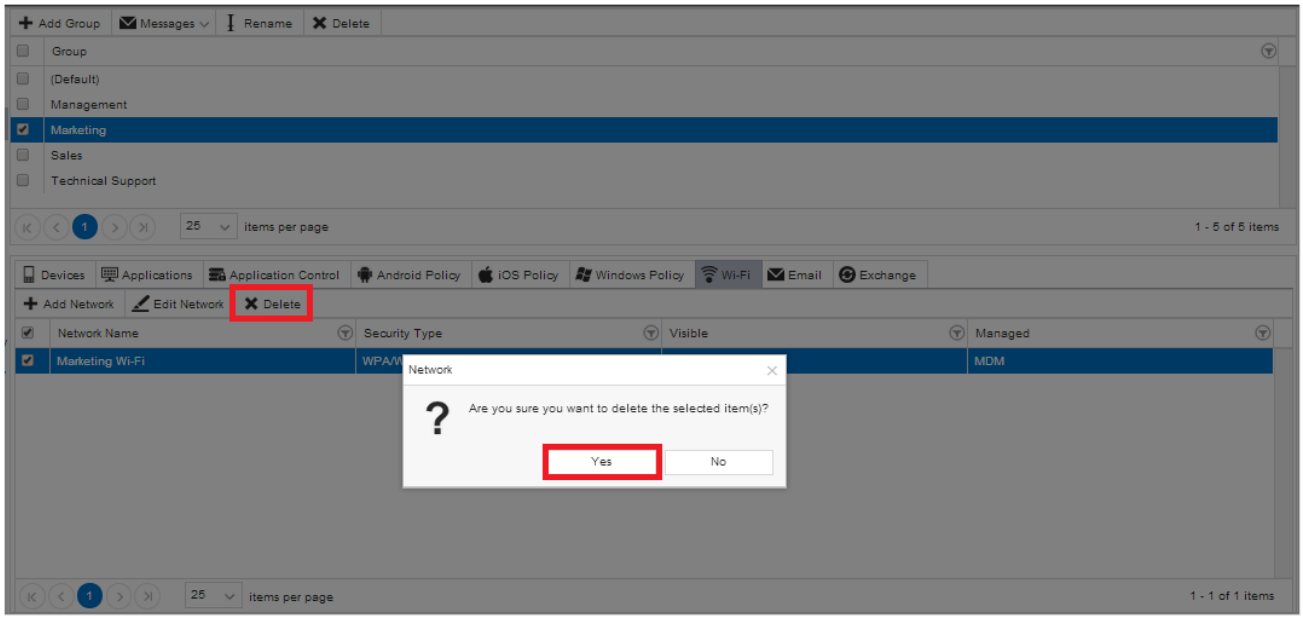


3. Click on the ‘Wi-Fi’ tab, select the network and press ‘Edit Network’.
4. Make your changes and press ‘Save’.

Deleting Wi-Fi Networks from Multiple Devices

To remove a Wi-Fi network from a group of devices:

1. Click on ‘Group Policies’.
2. Select the group and click on the ‘Wi-Fi’ tab.



3. Select the network to delete and press the ‘Delete’ button.
4. Press ‘Yes’ at the confirmation dialog and you will receive a confirmation message.
5. Click ‘OK’ to clear the dialog.

Remote Control

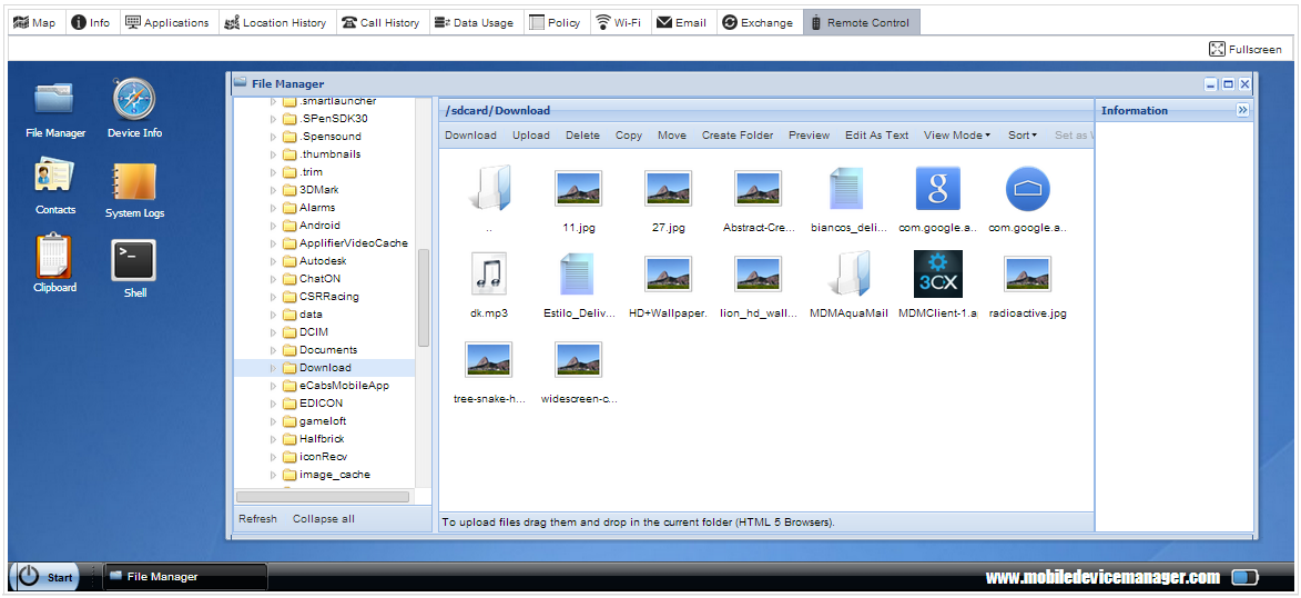
Introduction

Mobile Device Manager allows you to remotely control mobile devices. This feature is currently only available for Android devices. With the remote control function you can login to the device from anywhere and perform many administrative functions, such as file management, apps management and issue commands and more.

Remote File Management

The Remote Control tab allows you to access the built in file manager and manage the files on the device remotely through the MDM portal. To access the file manager:

1. Select the device from the 'Devices' node.
2. Click on the 'Remote Control' tab.
3. Once the remote control module loads click on 'File Manager'.



The file manager allows you to browse through your Android device's folders and offers the following functions to the user:

1. Downloading files from the mobile device to the computer.
2. Uploading files from the computer to the mobile device.
3. Delete, Create, Copy and Paste actions for files and folders.
4. File Preview.
5. Text Editing.
6. Sorting and Viewing modes.

Note: Currently for privacy reasons access to the photo folder is prohibited.

Other Administrator functions

In addition to the File Manager the following functions are available to the user:

Remote Shell

This allows you to use commands to access the Android's OS inner workings. The terminal uses unix like commands and is especially useful for developers/ programmers as it allows you to fix

android devices remotely, push, pulls applications onto a phone, configure directory access and anything in between.

System Logs

Allows you to view the device system logs. The Android OS uses a logging system that keeps a record of what actions the Android OS and the applications are doing on your device or on other devices. Very useful for debugging or tracing the source of problems.

Device Info

Provides real time information about the status of your Android smartphone including, its IP Address, Battery charge and status, Memory status, Network Connectivity details and type, Operator details and sim serial numbers and phone sensor information.

Contacts

Provides a method of remotely administering your device contacts, allowing you to review, filter, remove and edit already existing contacts, or push a new contact to the device altogether.

Clipboard

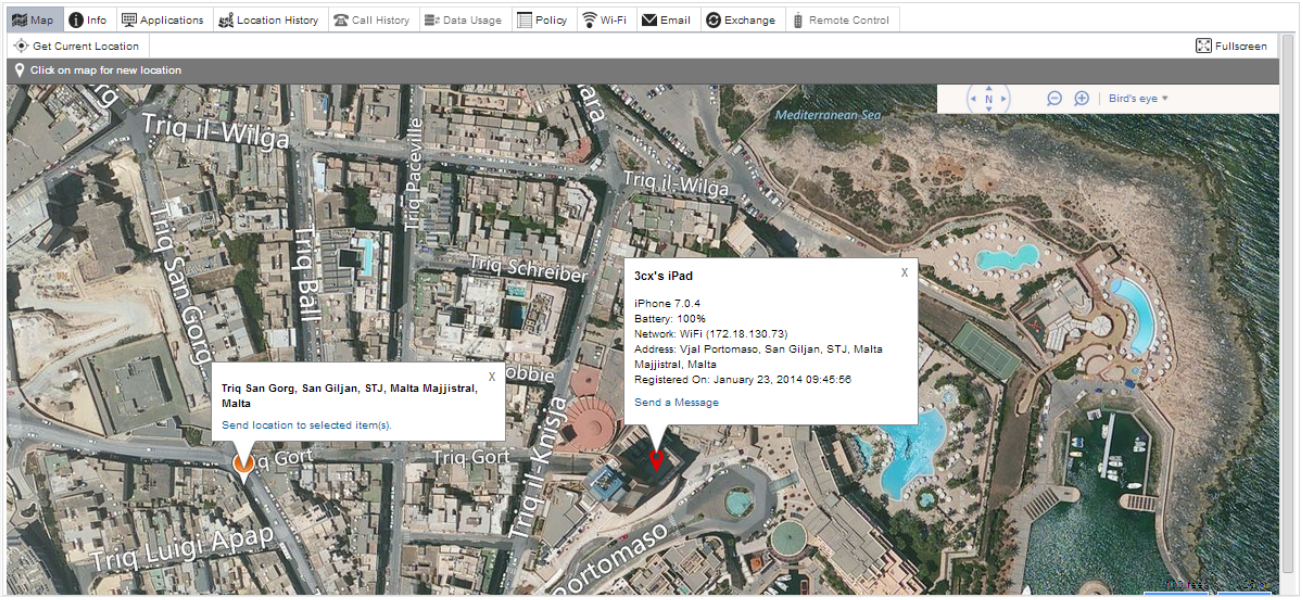
Review text currently set in the Android device clipboard and further alter this text or input new text altogether.

Messages and Directions

Introduction

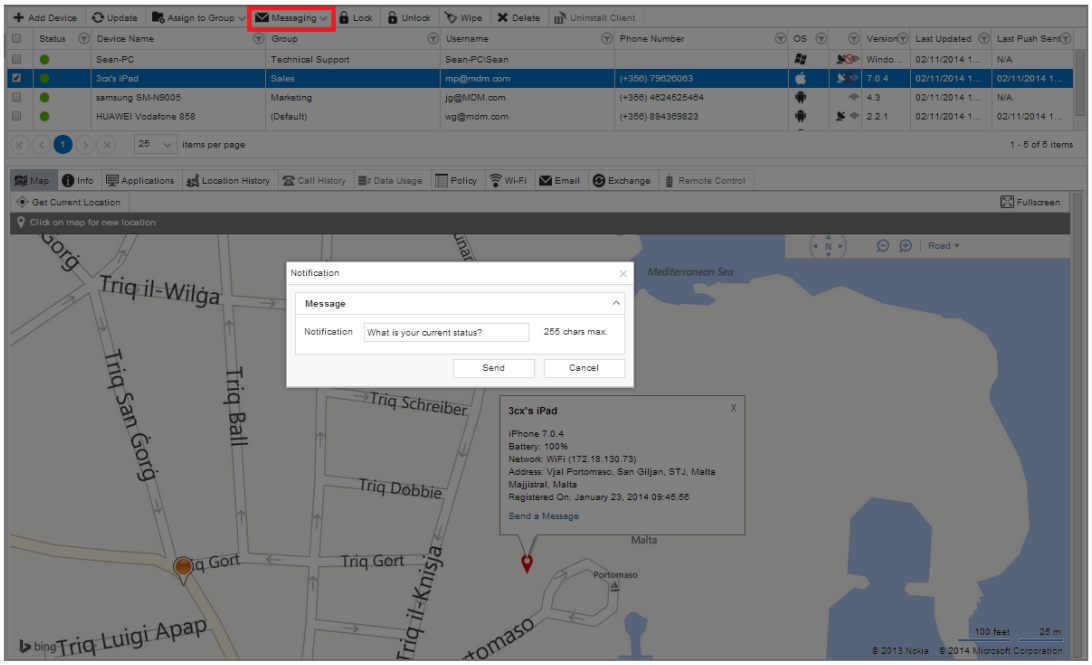
Mobile Device Manager includes a messaging functionality that allows messages to be sent to all devices, to a group of devices or just to a particular device.

Send Directions



In addition to standard text messages, admins can send a location on Google Maps to a device. When the recipient opens the message, the location is displayed on the phones Google Maps app, allowing them to easily navigate to it.

Send Text Messages

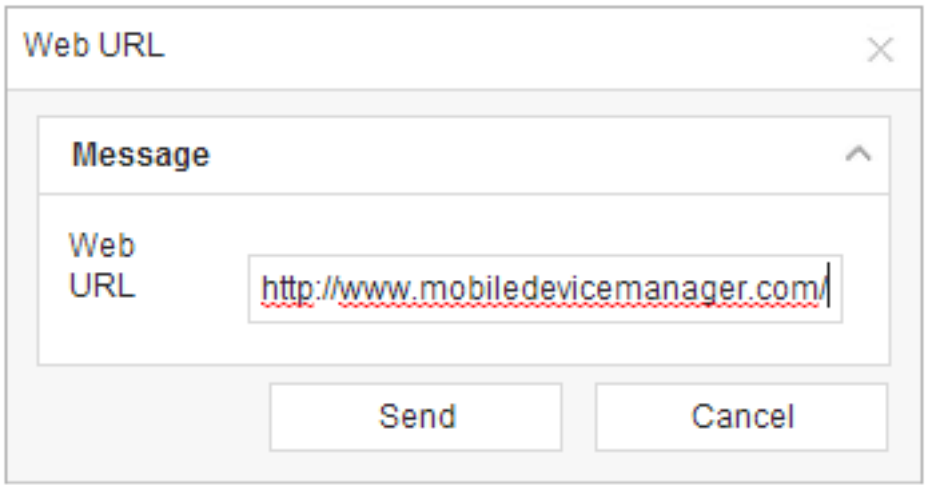


In order to send a text message to the device you have to do this:

1. Go to the ‘Devices’ node and select the device that you want to message.
2. Click the ‘Messaging’ option located to the middle of the top bar above the device list and select ‘Notification’.

3. Type your message in the notification field dialogue box (shown in the Image above).
4. Press ‘Send’ to send your message to the device.

Send Web URL Messages

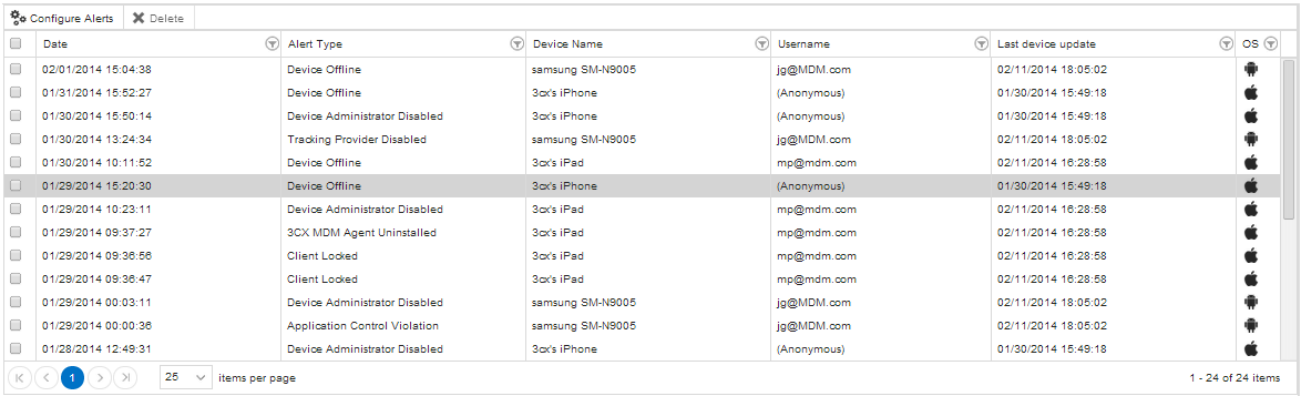


Select the ‘Send Web URL’ option to push out a web page to selected devices by according to the next steps.

1. Click ‘Send Web URL’.
2. Enter a URL into the Web URL text field (ex. http://www.mobiledevicemanager.com/).
3. Click ‘Send’ to send the URL message to the selected device/ devices.

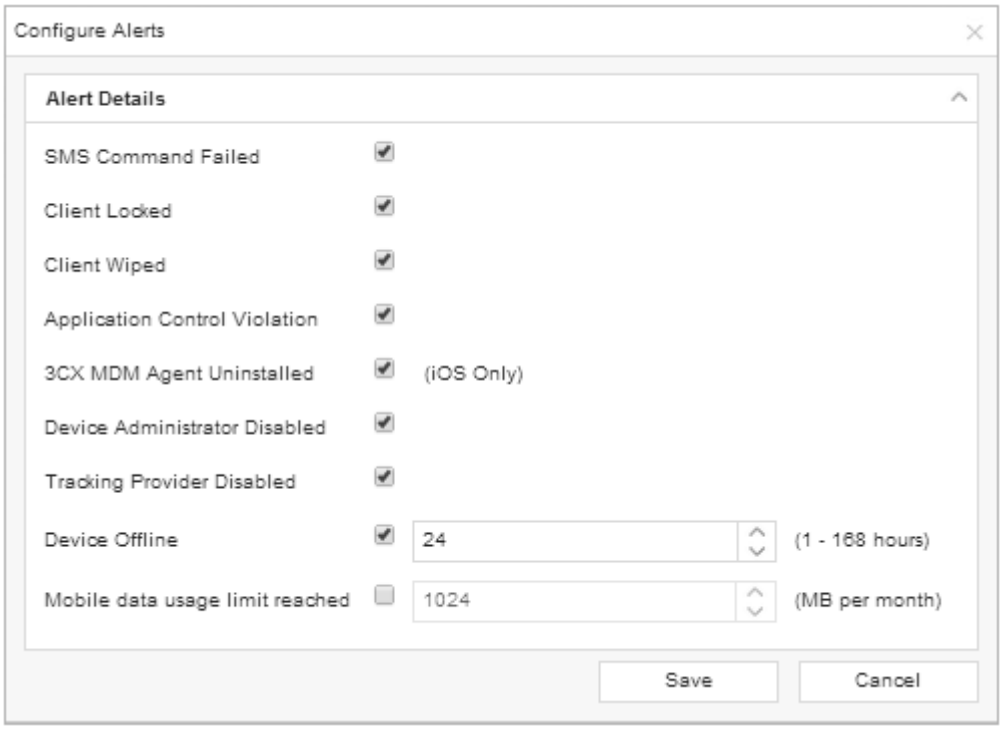
Alerts

Introduction



The ‘alerts’ node allows administrators to be alerted for important events. Alerts are listed in the alerts node, but will also be sent by email to the administrator’s email address. You can configure your alerts by going to the Alerts node >Configure Alerts.

Alerts Available



The following alerts are currently available in Mobile Device Manager and are configurable by the MDM administrator:

- **SMS Command Failed** - Sent when sending a lock or wipe via SMS fails due to incorrect phone number or a network provider which is not supported.
- **Client Locked** - Sent when a client lock command is completed.
- **Client Wiped** - Sent just before the device executes a wipe.
- **Application Control Violation** - Sent when a user installs an application which is blacklisted or an application which is not whitelisted according to the policy specified by the group.
- **MDM Agent Uninstalled** - iPhone only - Sent when the MDM app is uninstalled.

- **Device Administrator Disabled** - Sent when the user disables device administrator on Android or when the user uninstalls the Configuration profile on iPhone.
- **Tracking Provider Disabled** - Sent when the user disables location tracking.
- **Device Offline** - Sent when a device is offline for more than x hours.
- **Mobile data usage limit reached** - Sent when the specified amount of data per month limitation is exceeded.

System Node (Advanced Settings)

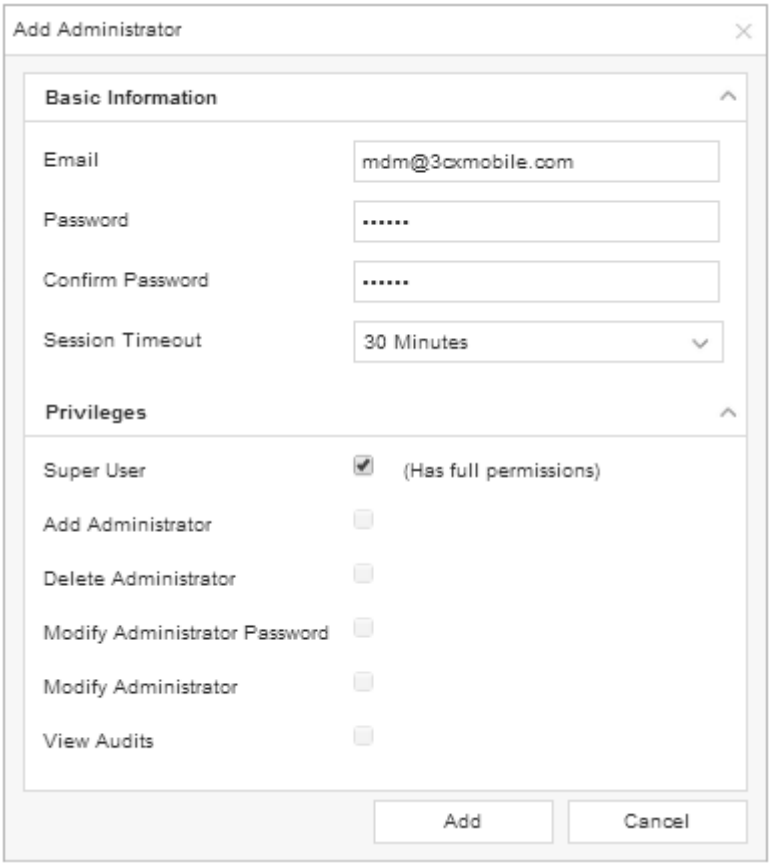
Introduction

The System node includes all settings relating to your account.

Administrators

You can configure multiple administrators for your account that are able to manage your mobile devices. All administrator actions are logged, and the audit trail can be viewed from the ‘Auditing’ node.

To add new administrators to your account press the ‘New Administrator’ button and fill in the new administrator’s details and privileges.



Basic Information:

- Email: The new administrator’s email account
- Password: The password that the new admin will use to log into the account
- Confirm Password: Same as above
- Session Timeout: Time limit in which if no action is taken the admin will be logged out.

Privileges:

These settings specify what the new admin can and cannot do

- Super User: Has full permission to do anything
- Add Administrator: Can add another administrator
- Delete Administrator: Can delete administrators
- Modify Administrator Password: Can change administrator passwords
- Modify Administrator: Can modify administrators settings
- View Audits: Can view the Audits from the audit node.

Deleted

This node contains the devices that were deleted from your account and offers you a chance to recover them or delete them completely.

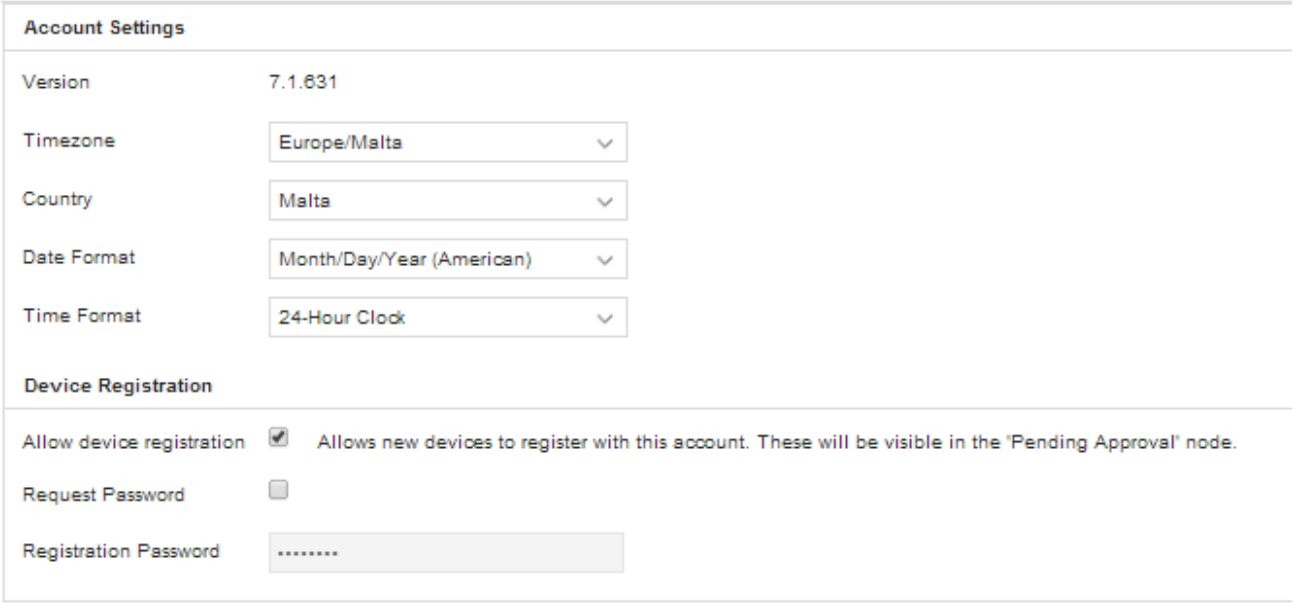
Auditing

This node shows information about the admins logging in and out of your account such as the date, time that they logged in and out, and the admin name.

Apple Certificate

The Apple Certificate node allows you to Renew your apple certificate or disable the iOS device Management completely by clicking the appropriate button

Account Settings



This node allows you to specify how devices get enrolled to your mobile device management account. You can choose to approve each device that requests to be enrolled to your account, or you can set a password that the user will enter, so that the approval is automatic.

The time zone, country, date and time format can also be set from this node.